IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

IN RE: DEALER MANAGEMENT
SYSTEMS ANTITRUST LITIGATION

This Document Relates To:

Authenticom, Inc. v. CDK Global, LLC, et al.,
Case No. 1:18-cv-00868 (N.D. Ill.)

MDL No. 2817
Case No. 18-cv-00864

Hon. Robert M. Dow, Jr.
Magistrate Judge Jeffrey T. Gilbert

PUBLIC-REDACTED

PLAINTIFF AUTHENTICOM, INC.'S REPLY IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT ON DEFENDANTS' COUNTERCLAIMS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

RULES

Fed. R. Civ. P.:

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

GLOSSARY

Abbreviation	Title	Dkt.
ACOM SUF	Plaintiff Authenticom, Inc.'s Statement of Undisputed Material Facts in Support of Its Motion for Summary Judgment on Defendants' Counterclaims (May 20, 2020)	Dkt. 977
ACOM RSUF	Plaintiff Authenticom, Inc.'s Responses to Counterclaimant's The Reynolds and Reynolds Company's Statement of Undisputed Material Facts in Support of Its Motion for Partial Summary Judgment (July 28, 2020)	Dkt. 1082
DJ SAF	Defendants CDK Global, LLC's and The Reynolds and Reynolds Company's Statement of Additional Material Facts in Opposition to MDL Plaintiffs' Motions for Summary Judgment on Defendants' Counterclaims (July 28, 2020)	Dkt. 1062
DJ SUF	Defendants CDK Global, LLC's and The Reynolds and Reynolds Company's Joint Statement of Common Undisputed Material Facts in Support of Their Motions for Summary Judgment (May 20, 2020)	Dkt. 974
PJ RSAF	MDL Plaintiffs' Responses to Defendants CDK Global, LLC's and The Reynolds and Reynolds Company's Statement of Additional Material Facts in Opposition to MDL Plaintiffs' Motions for Summary Judgment on Defendants' Counterclaims	Filed concurrently
PJ SAF	MDL Plaintiffs' Corrected Statement of Additional Material Facts in Opposition to Defendants' Motions for Summary Judgment (July 28, 2020)	Dkt. 1101
PJ RSUF	MDL Plaintiffs' Responses to Defendants CDK Global, LLC's and The Reynolds and Reynolds Company's Joint Statement of Common Undisputed Material Facts in Support of Their Motions for Summary Judgment (July 28, 2020)	Dkt. 1070
Resp. ACOM SUF	Response of Defendants CDK Global, LLC and The Reynolds and Reynolds Company to Plaintiff Authenticom, Inc.'s Statement of Undisputed Material Facts In Support of Its Motion for Summary Judgment On Defendants' Counterclaims (July 28, 2020)	Dkt. 1058

Abbreviation	**Title**	**Dkt.**
RSUF	Counterclaimant The Reynolds and Reynolds Company's Statement of Undisputed Material Facts in Support of Its Motion for Partial Summary Judgment (Oct. 15, 2019)	Dkt. 779
Dealers' Ex.	Exhibits to the Declaration of Peggy J. Wedgworth (May 20, 2020)	Dkt. 958-1
Dorris Ex.	Authenticom Exhibits to the Declaration of Daniel V. Dorris (May 20, 2020)	Dkt. 977-1
Fenske Ex.	Exhibits to the Declarations of Daniel T. Fenske (May 20, 2020 & July 28, 2020)	Dkts. 975, 979, 1064 & 1065
Ho Ex.	MDL Plaintiffs' Exhibits 1-503 to the Declaration of Derek T. Ho (July 28, 2020); and MDL Plaintiffs' Exhibits 504-521 to the Declaration of Derek T. Ho (Aug. 28, 2020)	Dkt. 1069-1 & filed concurrently
Wedgworth Ex.	Exhibits to the Declaration of Peggy J. Wedgworth (July 28, 2020)	Dkt. 1083
Wilkinson Ex.	Exhibits to the Declaration of Brice Wilkinson (July 28, 2020)	Dkt. 779-1

INTRODUCTION

Defendants' counterclaims seek to impose ruinous liability on Authenticom – literally billions of dollars – for supposedly accessing their DMS without authorization. Defendants never brought any of these claims against Authenticom until Authenticom had the audacity to sue them for serious antitrust violations – even though they knew Authenticom had been accessing their DMSs for close to a decade. For good reason, as it turns out: Defendants' contracts with dealers gave dealers' agents license to access the DMS, and the undisputed evidence shows that Authenticom was dealers' agent. Defendants' effort to rewrite that license fails as a matter of law, and their attempt to dispute Authenticom's agency status relies on facts that are immaterial under settled agency law. Independently, Defendants' opposition brief confirms that their DMCA and CFAA counterclaims contravene the plain language of those statutes and that they lack evidence of several other essential elements of their claims. Defendants should not be permitted to distract the jury from their anticompetitive conduct with their extravagant but legally defective claims. Summary judgment for Authenticom should be granted.[1]

ARGUMENT

I. Defendants' Counterclaims Fail Because Authenticom's Access Was Authorized

A. Defendants' DMS Licensing Contracts Permit Access By Dealers' Agents

Defendants' DMS licensing contracts with dealers permit dealers' "agents" to access and use the DMS. The undisputed evidence now establishes that Authenticom's access was authorized because it acted as dealers' agent in accessing the DMS on their behalf.

[1] Capitalized terms are defined in Authenticom's summary judgment brief (Dkt. 978).

1. Authenticom Did Not Judicially Admit Lack Of Authorization

Defendants attempt to sweep the evidence of Authenticom's authorization under the rug by contending that Authenticom admitted lack of authorization when it alleged that CDK and Reynolds forced dealers to accept "contractual terms" that "prohibit dealers from granting access to their data" to third parties "such as Authenticom." *Authenticom* Dkt. 1 ¶ 150. That argument is wrong, because (1) Authenticom's *legal* assertion does not constitute a *factual* admission; (2) Defendants' responses to that allegation mean it cannot bind Authenticom; (3) in the case of Reynolds, discovery revealed facts inconsistent with Authenticom's prior legal assertion; and (4) CDK has long been aware that Authenticom took the position that its access to CDK's DMS was contractually authorized.

First, the allegation in question – that Defendants' contracts prohibited dealers from authorizing third parties like Authenticom to access Defendants' DMS – relates to a matter of law (the interpretation of Defendants' contracts); accordingly, the rule that *factual* allegations are binding on the party in subsequent proceedings does not apply. Defendants' argument "relies on a misunderstanding of the nature of judicial admissions, which are statements of fact rather than legal arguments made to a court." *New York State Nat'l Org. for Women v. Terry*, 159 F.3d 86, 97 n.7 (2d Cir. 1998); *see also Solon v. Gary Cmty. Sch. Corp.*, 180 F.3d 844, 858 (7th Cir. 1999) (judicial admissions "have the effect of withdrawing *a fact* from contention") (emphasis added).[2] Defendants' cases confirm the point: they all involve admissions as to issues of *fact*, not legal questions of contract interpretation.[3]

[2] *See Dabertin v. HCR Manor Care, Inc.*, 68 F. Supp. 2d 998, 1000 (N.D. Ill. 1999) ("It is well established that judicial admissions on questions of law have no legal effect."); *In re TK Boat Rentals, LLC*, 411 F. Supp. 3d 351, 368 (E.D. La. 2019) (similar).

[3] *See, e.g.*, *Conrad v. Bendewald*, 500 F. App'x 526, 528 (7th Cir. 2013) (use of video); *Monumental Life Ins. Co. v. Ill. Mut. Life Ins. Co.*, 2012 WL 5845631, at *2 (N.D. Ill. 2012) (date of retirement).

Indeed, Defendants have conceded the legal nature of these allegations: CDK responded to them by pleading that they "state[] *legal conclusions* to which no answer is required" and that "the contracts speak for themselves," Dkt. 229 ¶¶ 150-151 (emphasis added); Reynolds pleaded that "the referenced *documents . . . speak for themselves*," Dkt. 225 ¶ 152 (emphasis added). And this Court, in denying Authenticom's motion to dismiss CDK's counterclaim, noted that Authenticom's "characterization of the contract" could be treated as a "legal" issue. *See* Dkt. 506, at 12 n.3.[4] Notably, CDK did not argue – and the Court did not hold – that Authenticom's allegations were judicial admissions that would preclude it from asserting authorization, though the argument was just as available to CDK then as it is now.

To the extent the issue of Authenticom's authorization implicates a factual question, that question is whether Authenticom acted on behalf of dealers and subject to their control – the factual predicate for an agency relationship under Wisconsin law. *See infra* pp. 16-23. But there is no admission in Authenticom's complaint that Authenticom did not act on dealers' behalf or under dealers' control. To the contrary, Authenticom's complaint repeatedly alleges, in detail, facts establishing that Authenticom *did* act with dealer authorization and control.[5] There is thus no relevant factual admission at all – and the complaint as a whole does not so clearly disclaim the factual predicate for agency to satisfy the high standard for judicial admissions. *See, e.g.*, *JMS Dev. Co. v. Bulk Petroleum Corp.*, 2019 WL 8064002, at *5 (N.D. Ill. 2019) (judicial admission must be "deliberate, clear and unequivocal").

[4] Authenticom had a "good faith basis" for that allegation, Dkt. 506, at 12 n.3: CDK and Reynolds had told dealers that their contracts prohibited access by Authenticom.

[5] *See Authenticom* Dkt. 1 ¶ 55 ("Before a data integrator can pull data, it must get specific authorization from the dealer. For example, for integrators like Authenticom, dealers must set up separate login credentials for the integrators so that they can access the DMS database to pull the data."); *see also id.* ¶¶ 59, 78, 80 (allegations showing dealers authorize and control Authenticom's services).

Second, Authenticom had no reason to amend this allegation (even had it been factual, not legal) because both CDK and Reynolds took the position that these allegations were no longer operative on the ground that the legal claim they supported – for exclusive dealing – had been dismissed. The allegations in question were included in the complaint under the heading "CDK and Reynolds Require Dealers and Vendors to Enter into Exclusive Dealing Arrangements That Are Patently Anticompetitive." *Authenticom* Dkt. 1 ¶¶ 150-152. After the preliminary injunction proceeding and consolidation of this case for pretrial purposes in this MDL, the District Court (Judge St. Eve) dismissed Authenticom's exclusive dealing claim as it pertained to Defendants' contracts with dealers, and Authenticom did not replead it. *See* Dkt. 176. Subsequently, in its answer, CDK asserted that, as a result, "Plaintiff's claims and theories premised on CDK's contracts with its Dealer customers were dismissed by the Court and have not been repled." Dkt. 229 ¶¶ 11, 150-151. Reynolds made the same assertion in its answer. Dkt. 225 ¶¶ 11, 17-18, 150, 152. In light of Defendants' assertions, Authenticom had no reason to amend allegations in its *complaint* to preserve a legal argument relevant to its *defense* of Defendants' counterclaims. *Cf. Kelley v. Crosfield Catalysts*, 135 F.3d 1202, 1204-05 (7th Cir. 1998) ("If certain facts or admissions from the original complaint become *functus officio*, they cannot be considered by the court on a motion to dismiss the amended complaint."); *Thomas v. City of Philadelphia.*, 2020 WL 4334827, at *3 (E.D. Pa. 2020) (withdrawn pleading no longer operative).

Third, Reynolds cannot reasonably assert that those paragraphs of Authenticom's complaint constitute judicial admissions given that it *denied* those allegations. Reynolds's *denials* are no less judicial admissions – and no less subject to Rule 11 – than Authenticom's allegations. *See Am. Network Leasing Corp. v. Peachtree Bancard Corp.*, 1996 WL 451304, at *5 (N.D. Ill. 1996) ("Yet, Vicom *denied* this allegation in its amended answer to Peachtree's verified complaint.

Vicom's denial . . . is itself a judicial admission . . . .") (citation omitted). Given that Reynolds contested the truth of Authenticom's allegations in its own answer, its effort to pin Authenticom to its pleading – and ignore its own pleading – is unavailing. *See id.* (where allegations are denied, neither of the "competing judicial admissions" is dispositive).

Reynolds's citation (at 6-7) to Authenticom's preliminary injunction briefing is no more persuasive. The preliminary injunction motion was briefed before the dismissal of Authenticom's exclusive dealing claim, and before Defendants filed their answers. As to Reynolds in particular, because there was no discovery prior to the preliminary injunction hearing, Authenticom was limited to publicly available documents and those that Reynolds chose to put in the record. And Reynolds did not submit into evidence the Reynolds Defined Terms, which expressly defines "You" to include dealers' agents. *See infra* p. 10. Given that Reynolds withheld this pivotal provision, Authenticom did not knowingly and voluntarily waive its right to assert that its conduct was authorized. *See Bank of Ill. v. Allied Signal Safety Restraint Sys.*, 75 F.3d 1162, 1166 (7th Cir. 1996) (judicial admissions require "actual knowledge" of the fact at issue); *FDIC v. Frye*, 2016 WL 6270532, at *2 (C.D. Ill. 2016) ("The Seventh Circuit has explained that a judicial admission is akin to waiver, that is, 'a deliberate relinquishment of a known right.' ") (quoting *Higgins v. Mississippi*, 217 F.3d 951, 954-55 (7th Cir. 2000)). By the same token, the statements by Chief Judge Peterson and the Seventh Circuit regarding the Reynolds contract – at early stages of the litigation – were made without the benefit of the full contract, including the definitions.

Fourth, Authenticom did have full copies of the CDK DMS contract during the preliminary injunction proceedings, and it argued expressly that it permits agent access.[6] Unsurprisingly,

[6] Ho Ex. 511, PI Hr'g Tr. (Day 3) 46:6-9 (Authenticom's counsel arguing during closing arguments on June 28, 2017: "CDK's contract permits dealers to authorize agents to access data under the contract, and the dealers had done so with CDK's express approval until CDK changed its mind about whether that was economical in 2015."); *id.* at 69:19-20 (the Court noting "CDK allows its dealers to appoint agents to

Defendants do not argue they were surprised or prejudiced by a legal argument Authenticom has been making for more than three years. *See Frye*, 2016 WL 6270532, at *2 (rejecting judicial admission where party "cannot seriously contend that [it is] surprised or prejudiced"; waiver in such circumstances "reeks of formalism and runs counter to the Federal Rules' admonition to decide cases on their merits"). The parties' active litigation over this issue for three years is reason enough to reject Defendants' argument. *See Cooper v. Carl A. Nelson & Co.*, 211 F.3d 1008, 1014 (7th Cir. 2000) (trial court has discretion as to whether to treat an allegation in a party's pleading as a judicial admission); *Wilda v. JLG Indus., Inc.*, 2020 WL 3618685, at *15 (N.D. Ill. 2020) (judicial admissions are "not a vehicle for playing gotcha" and should not be deployed to "interfere with the overriding truth-seeking function of litigation").

2. Defendants' Contracts Permit DMS Access By Dealers' Agents

a. CDK now concedes – as it must, given the contract's plain language – that § 6(D) of the Master Services Agreement ("MSA"), *see* Fenske Ex. 64 (Dkt. 975-64), permits dealers' agents to access and use the DMS. *See* CDK Br. 8 (dealers' "'employees and agents' can still access the DMS"). CDK now argues instead that "the prohibition on third-party software that appears elsewhere in the contract" deprives Authenticom of authorization to *use its own software* to access CDK's DMS. *Id.* at 8-9 (citing MSA § 6(B) ("Client is not authorized to cause or permit any third party software to access the [DMS] except as otherwise permitted by this agreement.") (capitalization omitted)). CDK's interpretation of MSA § 6(B) is unpersuasive.

access its DMS"); *id.* at 100:5-6 (the Court: "It does seem that CDK allows the dealer to designate agents."); Ho Ex. 512, Authenticom Consol. 7th Cir. Br. 12-13 ("CDK's standard DMS contract states that a dealer's 'employees *and agents*' may 'have access' to the DMS.").

First, "agents" are not "third parties" under the contract, so dealers' use of Authenticom's software does not violate § 6(B).[7] One need look no further than § 6(D) itself. That provision, as CDK now concedes, permits DMS access by dealers' "employees and agents." But the very next sentence states: "Client shall not allow access to any CDK Products by any third parties except as otherwise permitted by this Agreement." Access by "agents" is allowed; access by "third parties" is not. The two terms clearly have different meanings. *See Woods v. Elgin, Joliet & E. Ry. Co.*, 2000 WL 45434, at *5 (N.D. Ill. 2000) ("When parties to a contract use different terms to address similar issues, it is reasonable to infer that they intend these terms to have different meanings.").[8]

To read "third party software" in § 6(B) to include "agents' software" would inappropriately give "third party" in § 6(B) a different meaning than in § 6(D). *See Chi. Home for Girls v. Carr*, 133 N.E. 344, 346 (Ill. 1921) ("Words used in one sense in one part of a contract are, as a general rule, deemed to have been used in the same sense in another part of the instrument, where there is nothing in the context to indicate otherwise."); *Comm'r v. Keystone Consol. Indus., Inc.*, 508 U.S. 152, 159 (1993) (same principle). CDK offers no justification for reading "third parties" in § 6(D) to *exclude* agents, while reading "third party" in § 6(B) to *include* agents. CDK's contention (at 9) that agents can sometimes be referred to as "third parties" in other contexts misses the point. The relevant question is the interpretation of those terms as used *in the MSA*. So, too, does CDK's argument (at 7-8) that the "ordinary meaning" of "third party" includes agents. Given that an agent acts on behalf of the dealer, for the dealer's benefit, it is hardly clear that dealers'

[7] There is no factual dispute that Authenticom uses its own software – not "third party software" – to access and use the CDK DMS. *See* PJ RSAF 17, 22.

[8] CDK relies on *Avondale Industries, Inc. v. International Marine Carriers, Inc.*, 15 F.3d 489, 494 (5th Cir. 1994), but that case was not trying to reconcile two distinct contract terms. Rather, the court merely observed that a party could qualify as a "subcontractor," as defined in the contract, regardless of whether their real-world conduct established an agency relationship.

agents fall within any "ordinary meaning" of "third parties." At any rate, because the MSA's terms draw a clear distinction between "agent" and "third party," they must be given distinct meanings.

Second, even if "third party software" in § 6(B) were properly read to include "agents' software," § 6(B) contains a proviso that third-party software is prohibited "except as otherwise permitted by this agreement." Section 6(D) provides that permission because it expressly authorizes dealers' agents to access and use the DMS, without any limitation as to whether those dealer agents can use their own software to access the DMS.

CDK's argument (at 8) that § 6(B) is more specific than – and therefore controls over – § 6(D) is off the mark. To begin with, that canon cannot apply because § 6(B) expressly states that it yields to other provisions of the agreement, so § 6(D) would control over § 6(B), not vice versa. But, in any event, the canon applies only where there is ambiguity in the contract because irreconcilably conflicting provisions address the same topic. *See, e.g.*, *Bank of Commerce v. Hoffman*, 829 F.3d 542, 548 (7th Cir. 2016) ("[W]here an ambiguity exists in a contract due to a conflict between two of its provisions, the more specific provision relating to the same subject matter controls over the more general provision."); *Insignia/Frain Camins & Swartchild v. Querrey & Harrow, Ltd.*, 36 F. Supp. 2d 1051, 1055 (N.D. Ill. 1999) (rejecting interpretation that would "render the more specific provision . . . meaningless") (cited by CDK at 8). Where two provisions can be harmonized, courts should do so.[9] Here, there is no "conflict" between § 6(B) and § 6(D): a dealer may use agents (and agents' software) to access the DMS (per § 6(D)), but neither dealers nor their agents may obtain that access using third-party software (per § 6(B)). Unlike CDK's

[9] *See Sloan Biotechnology Labs., LLC v. Advanced Biomedical Inc.*, 101 N.E.3d 141, 151 (Ill. App. Ct. 2018); *Lincoln Elec. Co. v. St. Paul Fire & Marine Ins. Co.*, 210 F.3d 672, 685 (6th Cir. 2000) (Ohio).

interpretation, Authenticom's reading gives the terms "agents" and "third parties" distinct meanings without rendering either term superfluous.[10]

Third, Authenticom's interpretation does not negate MSA §§ 11, 9(B), or 5(F). *See* CDK Br. 10. By their terms, those provisions together govern instances in which the dealer wishes to *install* additional software or equipment on the CDK DMS.[11] There is no allegation that Authenticom ever installed equipment, and so § 9(B) and the corresponding portions of § 11 are irrelevant. As to software, these provisions concern only "Onsite implementation[s]" – meaning ones where the CDK DMS is physically located in the dealership. *See* Fenske Ex. 529 (Dkt. 1065-61), Stroz Rep. ¶ 37 (noting these were phased out in 2008 and 2009). Those provisions thus apply to installing software on CDK DMS servers at the dealership – which CDK calls "code on the box" and claims is a longstanding concern. PJ RSUF 59. It is undisputed that Authenticom does not put "code on the box." *Id.*; Wedgworth Ex. 4 (Dkt. 1083) at 1-A-111:5-8. Rather, Authenticom employs "user emulation," ACOM SUF 27, which uses the *DMS software* to extract or write back data just as a dealership employee would, *see* Dorris Ex. 9 (Dkt. 977-10), ¶ 6 (dealership IT director: Authenticom "pull[s] the exact same data that I could myself (or one of my employees could) pull"). In any event, these provisions *allow* such software or equipment to be installed if

[10] Contrary to CDK's argument (at 9), this construction does not drain § 6(B) of independent meaning. Were it not for § 6(B), dealers and their agents would be allowed under § 6(D) to use any software to access the DMS. Notably, moreover, neither CDK's nor Reynolds's DMS contract bans dealers from using automated methods of access. ACOM SUF 109 (CDK acknowledging the dealer can use "automated means" to run the DMS software); *Authenticom, Inc. v. CDK Glob., LLC*, 2017 WL 3017048, at *9 (W.D. Wis. 2017) (Reynolds's DMS contracts "do not specifically prohibit automated access, if done by the dealers or their employees"). Given that agents act on dealers' behalf, it is hardly anomalous that the MSA would permit dealers to use agents' software to obtain automated access.

[11] *See* Dorris Ex. 16 (Dkt. 977-17), at -149-150, § 5(F) (with respect to an "Onsite implementation," the dealer can "request" that CDK "approve" the addition of third-party software to the CDK DMS); *id.* at -153, § 9(B) ("Client shall have the option of obtaining additional equipment . . . from any third party"): *id.* at -155, § 11(A) (setting procedure for resolving the dealer's request for addition of third-party "Client Software or equipment," including in the event CDK "reasonably believes" that software or equipment will cause service or performance issues).

the dealer satisfies CDK that the software or equipment will not "degrade the performance" of the DMS. Dorris Ex. 16 (Dkt. 977-17), at -155, § 11(A). These provisions are therefore fully consistent with Authenticom's access being authorized.

[redacted] *See* Fenske Ex. 64 (Dkt. 975-64), MSA § 18(A) ("This Agreement shall not be modified in any way except by a writing signed by *both parties*.") (emphasis added). Nor does that imply that other CDK dealers lacked those rights. *See Spectrum Health–Kent Cmty. Campus v. NLRB*, 647 F.3d 341, 346 (D.C. Cir. 2011) ("drafters of contracts do sometimes take a belt-and-suspenders approach").

b. Reynolds's argument (at 8-11) that only dealer employees are licensed to use or access the Reynolds DMS cannot be right because it reads out the words "agents and representatives" from § 1 of the Master Agreement. The first paragraph of § 1 of Reynolds's Master Agreement expressly states: "LICENSES. You . . . may Use the Licensed Matter . . . for the internal data processing needs of your automotive business." *See* Dorris Ex. 19 (Dkt. 977-20), at -044, § 1. The Defined Terms expressly defines the capitalized terms therein: (1) the "Licensed Matter" includes the DMS software; (2) "Use" means to "copy[ ]" the Licensed Material onto computer hardware "for processing of the instructions or statements contained" therein; and (3) "You" means not only the dealership itself but also "all of [its] employees, agents, and representatives." Dorris Ex. 21 (Dkt. 977-22), at -679 (Reynolds Defined Terms). Those definitions are central to the proper interpretation of the contract. *See, e.g.*, *Bauer v. Int'l Bhd. Elec. Workers Local No. 150 Pension Fund*, 2014 WL 273887, at *4 (N.D. Ill. 2014) (St. Eve, J.)

("A basic principle of contract interpretation is that the court will apply definitions for defined terms."); *cf. Stenberg v. Carhart*, 530 U.S. 914, 942 (2000) (in statutory construction, courts "must follow [the legislature's] definition, even if it varies from that term's ordinary meaning").

Applying those definitions, § 1 of the Master Agreement plainly confers on dealers' agents a license to extract data from Reynolds's DMS on dealers' behalf. Reynolds's contrary interpretation directly conflicts with that language. *See BKCAP, LLC v. CAPTEC Franchise Tr. 2000-1*, 572 F.3d 353, 362 (7th Cir. 2009) ("[C]ourts must . . . give effect to every word, phrase, and clause in a contract and avoid an interpretation that would render any part of the contract surplusage or nugatory.") (alterations in original); *Shanesville Invs. LLC v. Eclipse Res. I, LP*, 358 F. Supp. 3d 665, 675 (S.D. Ohio 2018) (same under Ohio law).

Reynolds (at 10-11) dismisses these provisions as "generic language" that should yield to more specific provisions. But § 1 cannot be dismissed as a throw-away. It is the "LICENSES" – the first and foremost provision of the DMS contract. And the Defined Term "You" sets forth, with specificity, who is contractually entitled to that license. This is a term that Reynolds – as the drafter of the license agreement – surely considered with care.[12] Whatever the scope of the "specific-trumps-general" canon, it does not justify abrogating a term as central to the licensing agreement as the definition of the licensee.

At any rate, the other provisions Reynolds invokes are not inconsistent with the LICENSE provision of § 1 of the Master Agreement. Reynolds cites subsequent language stating that "You agree . . . not to disclose or provide access to any Licensed Matter or non-public portions of the Site to any third-party, except your employees who have a need for access to operate your

[12] *See, e.g.*, Corp. Counsel's Guide to Software Transactions § 2:33 (updated Apr. 2020) ("As in any software license, the precise definition of the licensee is very important. The contract must state exactly who is authorized to make the copies."); H. Ward Classen, *Fundamentals of Software Licensing*, 37 IDEA J.L. & Tech. 1, 6 (1996) ("Licensee" definition "is quite important for both financial and legal reasons.").

business," Dorris Ex. 19 (Dkt. 977-20), at -044, § 1, but its argument ignores context. The two sentences in question appear in different paragraphs of § 1. The first paragraph relates to the "LICENSES" to "Use" the DMS and expressly authorizes dealers and their "employees, agents, and representatives" to do so. The second paragraph relates to protection of Reynolds's intellectual property rights in the Licensed Material outside the context of "Use" of the DMS. That is clear from the second paragraph's first sentence, which refers to Reynolds's "proprietary rights in the Licensed Matter and the Site, Including [sic] copyrights, patents, and trade secrets." Thus, the provision that "You agree . . . not to disclose or provide access" to the DMS to third parties does not override the LICENSE provided in the first paragraph. Restrictions on *disclosure* of the Licensed Material should not be read to restrict "Use" of those materials.[13] *See also Lincoln Elec.*, 210 F.3d at 685 (provisions must be harmonized).

The confidentiality provision of the Customer Guide that Reynolds invokes (at 10 & n.5) likewise does not support its position. *See* Dorris Ex. 137 (Dkt. 977-139), at -266 to -268. To begin, the confidentiality section of the Customer Guide *confirms* that the licensee – "You" – includes agents, because it opens by stating that "'Confidential Information' means information disclosed by Reynolds . . . *to you or your agent or representative* in connection with the . . . use or operation of the Site." *Id.* at -266 (emphasis added). Reynolds simply ignores this provision. The later sentences of the confidentiality provision that Reynolds does cite relate, as with the second

[13] Also, given that the Defined Terms expressly defines "You" to include dealers' agents, the undefined term "third party" cannot be read to include such agents. Although Reynolds urges (at 5) that the Court infer that "third party" includes agents because of the exception for employees, any such inference cannot override the contract's plain language. *See, e.g., DeJohn v. The .TV Corp. Int'l*, 245 F. Supp. 2d 913, 923-24 (N.D. Ill. 2003) (adopting plain language where it "contradicts" interpretation supported by "inference"). At the very least, it is not clear that "third party" includes "agents," and that ambiguity must be construed against Reynolds, as the drafter of the agreement. *Cf. Supreme Laundry Serv., L.L.C. v. Hartford Cas. Ins. Co.*, 521 F.3d 743, 747 (7th Cir. 2008) (noting that the term "person" was ambiguous and construing it against the drafter).

paragraph of § 1 of the Master Agreement, to disclosure of Reynolds's intellectual property outside the context of use. At bottom, Reynolds's interpretation would require the Court to curtail the central "LICENSES" provision of the Master Agreement and ignore both the Defined Term "You" and several other terms of the Master Agreement and Customer Guide.

Reynolds's remaining arguments have no merit. *First*, Reynolds argues (at 12) that Authenticom exceeded the scope of the dealer's license by downloading copies of the "Reynolds's PC Software" – ERAccess and ERA-IGNITE – on Authenticom's servers. It relies on a provision in the third sentence of § 1 of the Master Agreement, which states that, "for Licensed Matter physically located at your location," the dealer is licensed to use "one copy of the object code of the Licensed Matter" "only" on the Reynolds-provided equipment at that location. Dorris Ex. 19 (Dkt. 977-20). That provision says that, where Reynolds has installed the DMS server on the dealer's physical premises, the dealer may use the DMS *server* software (the "object code" of the DMS server) only on that server. But there is no evidence that Authenticom copied Reynolds's *server* software – which is *not* the "PC Software" Reynolds refers to in its brief, *see* Fenske Ex. 107 (Dkt. 975-107), Hall 5/19/20 Decl. ¶¶ 2-4 – from Reynolds's servers onto its own computers.[14] Authenticom's conduct also satisfies the next provision of the third sentence of § 1, which provides that, "for Licensed Matter in a hosted environment," the dealer and its agents have a "subscription license to access and Use the Licensed Matter."[15] As explained above, Authenticom accessed and used Reynolds's DMS pursuant to that license in the same manner a dealership employee.

[14] The "object code of the Licensed Matter" referred to in this sentence is the DMS server software, not the client software. Reynolds's contrary reading – that the "object code of the Licensed Matter" includes the client-side software – cannot be correct because it is undisputed that dealers have authorization to run the "PC Software" on the dealers' own computers – not "only" on "Equipment" provided by Reynolds. *See* Fenske Ex. 19 (Dkt. 975-19), Hall 11/15/19 Decl. ¶ 5 (explaining "every" DMS installation includes "end-user application software on the *dealer's PCs*") (emphasis added).

[15] Reynolds's related argument (at 14) that "Use" means "copying any portion" of the Licensed Matter "into the specific unit of Equipment for which it is licensed" fails for the same reason. In § 1 of the

Second, Reynolds's invocation (at 12) of the restriction on "Other Matter" is inapplicable here because "Other Matter" is defined to be "any software [or] product . . . provided to you by a *third party*." Dorris Ex. 21 (Dkt. 977-22), at -679. Authenticom was an agent, not a third party.

Third, the prohibition on "reverse engineering" is irrelevant. "'Reverse engineering' is the process by which a person takes a legitimately acquired item, disassembles it to learn its component parts, and from that process determines how the product is manufactured," *Motorola, Inc. v. Comput. Displays Int'l, Inc.*, 739 F.2d 1149, 1152 n.4 (7th Cir. 1984), "typically with a view to manufacturing a similar product," *SAS Inst., Inc. v. World Programming Ltd.*, 874 F.3d 370, 381 (4th Cir. 2017). There is no evidence Authenticom had any interest in determining how the DMS was created or in creating a similar product.

Fourth, contrary to Reynolds's argument (at 14), Authenticom's "Use" of the DMS is for dealers' "internal data processing needs." Authenticom undisputedly processes data to support dealers' use of software applications they need to run their businesses. *See* Auth. Br. 8-10.

c. Buttressing the conclusion that Authenticom was authorized to access and use Defendants' DMSs as the dealers' agent, courts presume that copyright licenses – like the contracts here – grant an implied license for non-employee agents to use the license. *See* Auth. Br. 26; *see also Great Minds v. FedEx Office & Print Servs., Inc.*, 886 F.3d 91, 96 (2d Cir. 2018) ("Great Minds' licensees may rely on *non-employee* agents in carrying out permitted uses without converting those agents into independent licensees."). Given that presumption, Defendants bear the burden to show that their contracts preclude agent access; here, Defendants' arguments at best create ambiguity, which would leave the presumption of an implied license intact.

Master Agreement, the "Use" of Licensed Matter refers to use of the DMS server. Reynolds's contrary interpretation would prevent dealers from using "PC Software" on their own computers, which all parties agree is authorized.

Defendants have no persuasive answer to *Automation by Design, Inc. v. Raybestos Products Co.*, 463 F.3d 749 (7th Cir. 2006). There, the Seventh Circuit held that – notwithstanding the absence of any contractual authorization for agent use – the copyright licensee was nevertheless entitled to allow its agent to use the license (and hence copy the copyrighted material). *See id.* at 757 ("Once Raybestos secured the rights to duplicate the designs and 'use the license' to duplicate machinery, it could hire another party to manufacture parts for it if Raybestos lacked the tools or skills to do so itself."); *id.* at 758 ("[W]hatever rights Raybestos had to duplicate, it could hire PDSI to do so in its stead."). CDK's argument (at 23-25) that *Automation by Design* is different because of "intricacies" in the contract is not persuasive because the licensee here (the dealer) has express agent rights; if anything, the difference in contract language supports Authenticom.[16]

3. Defendants' Course Of Dealing Confirms The Dealers' Agent Rights

Because Defendants' DMS contracts unambiguously permit agents to access the DMS, the Court need not resort to extrinsic evidence or course of dealing to interpret the agreements. However, if the Court does review the parties' course of dealing, it confirms that both CDK and Reynolds have long permitted dealer agents to access the DMS.

CDK argues (at 18) that its course of dealing is "ambiguous" because it purportedly backed away from its public support of data integrators in 2012. That misstates the undisputed facts (based on CDK's own documents and witness testimony): [redacted]. But, regardless of the precise date CDK changed its policy, it had the same contract provisions that are now before the Court going back

[16] The fact that, in *Automation by Design*, the Seventh Circuit considered whether the copyright licensee had "transferred" the license to a third party makes no difference: the question there, as here, is whether the agent of the licensee is authorized to use the copyright license.

to at least 2008, ACOM SUF 54-58; hence, for many years, CDK construed its contracts consistent with the dealer's right to use data integrators as their agents.

With respect to Reynolds, there is no dispute that it knowingly "whitelisted" the ability of dealers to use data integrators [redacted] ACOM SUF 69-70; PJ SAF 27-28. Reynolds points (at 14-15) to its widely known *public position* against data integrators and threats to Authenticom, but what matters is Reynolds's course of *conduct*, which honored its closed-in-name policy in the breach and permitted dealers to use data integrators.

B. Authenticom Is The Dealer's Agent

When Authenticom provides data integration services, it does so "on behalf of [the dealer]" and "subject to control of" the dealer. *Lang v. Lions Club of Cudahy Wis., Inc.*, 939 N.W.2d 582, 590 (Wis. 2020). Under governing law, those facts establish that Authenticom is the dealer's agent. And there is no genuine dispute about those facts: Authenticom showed in its summary judgment motion (at 31-34) and supporting factual materials, *see* ACOM SUF 30-44, that dealers have the right to control Authenticom's access to the DMS and provision of data integration services from soup to nuts. Defendants' attempts to manufacture a factual dispute, despite this clear evidence, rely on a misreading of agency law and an improper attempt to elevate form (an alleged contract disclaimer) over substance (the reality of the parties' relationship). The Court should hold that Authenticom is the dealers' agent as a matter of law.

As a threshold matter, although Illinois law and Ohio law govern the analysis of CDK's and Reynolds's respective contracts, Wisconsin law governs whether Authenticom was the dealers' agent. As Authenticom explained (at 31 n.12) – and Defendants do not dispute – Wisconsin is where Authenticom enters into contracts with dealers and provides data integration services on their behalf. *See* Restatement (Second) of Conflict of Laws § 291 (1971). Regardless, choice-of-law here is immaterial because Defendants do not argue that Wisconsin agency law differs in any material respect from Illinois or Ohio agency law; all follow traditional common-law principles. *See* CDK Br. 18 (Wisconsin "is not an outlier on agency").[17]

As to the merits, Defendants largely ignore the substantial evidence – including statements by their own employees – that the defining feature of DealerVault is dealer control. ACOM SUF 30-44. The dealer not only authorizes and has the right to control Authenticom's access to the DMS (via dealer-provided login credentials), *see id.* 24-25, but it also determines in granular detail the data fields to which Authenticom has access, the frequency with which Authenticom accesses that data, and the vendors to which Authenticom sends that data, *id.* 26, 33-36. Defendants' quibbles with dealers' actual control over Authenticom's services cannot change the outcome because the analysis turns on the dealers' *right* to control, not on whether they always exercise that right. *See, e.g.*, *Lang*, 939 N.W.2d at 591 ("What matters in forming an agency relationship is that the principal has the right to control th[e] conduct."); *Sperl v. C.H. Robinson Worldwide, Inc.*, 946 N.E.2d 463, 471 (Ill. App. Ct. 2011) ("cardinal consideration is the right to control the manner of work performance, regardless of whether that right was actually exercised").[18]

Accordingly, the fact that one dealer testified he was "not curious" (CDK Br. 15-16) about Authenticom's technical process for extracting data does not defeat the agency relationship, because the dealer has the right to control Authenticom's ability to employ automated access

[17] Although Reynolds's contract *with dealers* has an Ohio choice-of-law provision, Authenticom is not a party to that contract (and has no contractual relationship with Reynolds). Because Reynolds made no attempt to explain why Authenticom, a non-signatory, would be bound by the choice-of-law provision in Reynolds's DMS contracts, it has waived any argument to that effect.

[18] *See also Am. Bullion, Inc. v. Regal Assets, LLC*, 2014 WL 6453783, at *3 (C.D. Cal. 2014) ("Actual control is not necessary[;] as long as there is an agreement that the principal has the right to control the agent, an agency relationship exists."); *In re FedEx Ground Package Sys., Inc., Emp't Practices Litig.*, 283 F.R.D. 427, 474 (N.D. Ind. 2008) ("an unused right to control remains a right to control for purposes of determining the nature of an agency relationship").

methods through dealer-created and -provided login credentials. ACOM SUF 24-26. Likewise, that Authenticom requests access to standard categories of data does not change that dealers have the right to control and limit the data categories (and data fields within those categories) that Authenticom can access. *Id.* 35, 40; Dorris Ex. 40 (Dkt. 977-41), Johnson Tr. 396:16-20 (dealer testifying: "[I]f there was something that [the vendor] didn't need, . . . I would uncheck it. And then on the next pull, those fields would no longer be – be selected and sent."). Reynolds's argument (at 18) that Authenticom controlled the timing and frequency with which it accesses the DMS fails for the same reason: dealers have the right to and do control and customize Authenticom's extraction times and frequency, even though Authenticom's standard practice is to pull data once daily after business hours if the dealer doesn't specify otherwise. ACOM SUF 36; Dorris Ex. 164 (Dkt. 977-166), Cottrell 5/19/20 Decl. ¶ 9 (within DealerVault, "dealers can choose to have Authenticom provide data integration services at multiple intervals during the day, once at night, once a week, or even once a month," and vary those intervals by vendor).[19]

Authenticom strongly disputes Defendants' inaccurate and spin-laden characterization (CDK Br. 17; Reynolds Br. 17-18) that Authenticom sold dealer data, without permission, to third parties. PJ RSAF 32. But, regardless, that argument is immaterial: Authenticom's involvement in the data venture cited by Defendants ended in 2012 (*see* CDK Br. 18), well beyond the statute of limitations for any of Defendants' counterclaims (except for its perfunctory unjust enrichment claim), Auth. Br. 62; and, regardless, it does not speak to whether dealers had the right to control Authenticom's access to and distribution of dealer data. As shown above, they did.

[19] CDK argues (at 16) that Authenticom used login credentials "interchangeably" to the "consternation of particular dealers," but CDK cites no factual support for that proposition (CDK cites to an exhibit dealing with an entirely different issue concerning CDK's contracts, *see* Fenske Ex. 69 (Dkt. 975-69). In any event, dealers create and control Authenticom's login credentials. ACOM SUF 24-26.

Defendants' argument (Reynolds Br. 17-18; CDK Br. 19-20) that dealers lack sufficient control over the technical "manner and method" of how Authenticom provides data integration services fails for two reasons. First, the undisputed facts show that dealers *do* have the right to control the technical manner in which Authenticom operates. For Authenticom to access the DMS through automated means, the dealer must create login credentials for Authenticom, which it has the power to revoke at all times, ACOM SUF 24-26; otherwise, the dealer must "push" the data to Authenticom – in which case Authenticom never has access to the DMS at all, PJ RSAF 35; PJ SAF 30; PJ RSUF 40.

Second, Defendants' argument that the dealer must control all the technical facets of Authenticom's services slices agency law too thin. The principal need not control *every* detail of the agent's work for an agency relationship to exist – as one of CDK's leading cases makes clear. *See Westmas v. Creekside Tree Serv., Inc.*, 907 N.W.2d 68, 77 (Wis. 2018) ("[A]n agent is one who acts on behalf of and is subject to *reasonably precise control* by the principal for the tasks the person performs within the scope of the agency.") (emphasis added); *see also Automation by Design*, 463 F.3d at 757 (rejecting attempt to "put[ ] too fine a point" on the agency analysis and finding agency existed where the principal hired the agent to "act in [its] stead").[20] Dealers need not reverse-engineer Authenticom's software (CDK Br. 13-14), choose the servers where DealerVault hosts data (*id.* at 16-17), or edit Authenticom's software scripts (Reynolds Br. 18) to establish an agency relationship – just as a client need not dictate how her attorney frames legal arguments. Here, all the "key" decisions are made by the dealer: whether, how, and how

[20] *See Great Minds*, 886 F.3d at 95 (finding FedEx was an agent of a school district, in context of a copyright license, and noting the "mundane ubiquity of lawful agency relationships"); *Delta Air Lines, Inc. v. Tie Cargo Corp.*, 1996 WL 1088913, at *2 (E.D.N.Y. 1996) (noting that "[e]very detail need not be determined by the alleged principal[ ] for an agency to exist"; rather, the principal must retain the right to control "policy" decisions and "key aspects of the undertaking") (citing cases).

frequently Authenticom can access the DMS; the data that Authenticom can access and extract; and where Authenticom sends that data. *See supra* p. 17; ACOM SUF 30-44. That goes far beyond a customer at a sandwich counter who only has a right to the finished product, as in CDK's hamburger analogy (at 15).

That vendors, not dealers, generally pay for Authenticom's service is true but irrelevant. *See* Reynolds Br. 16; CDK Br. 12. The principal need not pay the agent to establish an agency relationship. *See Giese v. Montgomery Ward, Inc.*, 331 N.W.2d 585, 597-98 (Wis. 1983) (agency relationship where father instructed son to mow the grass and had the right to control the task, even though it was "domestic chore" and no money exchanged hands). CDK's characterization (at 12) of vendors as Authenticom's "principal clients" – which is argument, not fact – does not affect Authenticom's agency relationship with the dealer so long as the dealer authorized and has the right to control the conduct alleged to cause injury (which, as explained above, they do). *See 1-800 Contacts, Inc. v. Lens.com, Inc.*, 722 F.3d 1229, 1250 (10th Cir. 2013) ("An agent can serve multiple principals at once, even principals that are competing with one another.") (citing cases).[21]

CDK's attempt (at 18-19) to distinguish *Lang* is unpersuasive. Although CDK argues that *Lang* "arose in an entirely different context" relating to recreational immunity, the Wisconsin Supreme Court construed the term "agent" according to its "plain meaning as a legal concept" by applying the "regular law of agency." 939 N.W.2d at 590, 591. The same task applies here.[22] The parties' contract in *Lang* referencing agency status did not dictate the court's analysis, because the

[21] CDK cites (at 12) an email exchange with the vendor Autobase, but that email (which is hearsay) illustrates the dealer's right to control Authenticom's services. *See* Fenske Ex. 427 (Dkt. 1064-72), at AUTH_004063673 ("As a DealerVault dealer, you can be assured that you have the visibility, security, and control you need to ensure only vendors that YOU want to share data with have access to your data.").

[22] CDK offers no statutory basis for its suggestion that, when the CFAA, the DMCA, or the Copyright Act are involved, a different test for agency applies. On the contrary, in *Automation by Design*, the Seventh Circuit applied the ordinary meaning of "agent" in the copyright context. 463 F.3d at 757.

substance of the relationship is what matters. *See infra* p. 22. And CDK misconstrues the facts of that case because the festival organizers (the Lions Club) did *not* provide specific instructions to its independent contractor with respect to the injury-causing conduct. *See* 939 N.W.2d at 587 ("During a deposition, Steven Fry explained that he had not received specific instructions from the Lions Club on how to lay electric and electronic cords."). An agency was nevertheless established because the festival organizers had the right to control the conduct, just as dealers have the right to control Authenticom's DMS access and data integration services. In *Westmas*, by contrast, the purported principal only "describe[d] the 'vision and concept' " for a tree-trimming project and said nothing at all about the safety precautions the vendor would use when performing the job. 907 N.W.2d at 79. That is a far cry from the facts here.

Reynolds misplaces reliance (at 16-17) on Ohio cases distinguishing between an employee and independent contractor. The factors relevant to establishing an employee relationship – such as whether the employer controls the employee's hours and provides the place of work and required "tools" – have no bearing on whether Authenticom is an agent. Most agents are independent contractors that would not qualify as an employee. *See, e.g.*, *Romero v. West Bend Mut. Ins. Co.*, 885 N.W.2d 591, 601-02 (Wis. Ct. App. 2016) ("Most of those we typically think of as agents – real estate agents, stockbrokers, and attorneys – are independent contractor agents."); *Braver v. NorthStar Alarm Servs., LLC*, 2019 WL 3208651, at *12 (W.D. Okla. 2019) ("The commercial world (not to mention the legal profession) abounds with independent contractor relationships that are also agency relationships."); *Tanksley & Assocs. v. Willard Indus., Inc.*, 961 F. Supp. 203, 207 (S.D. Ohio 1997) (similar). Reynolds is also wrong to suggest that Authenticom must establish a fiduciary relationship and the ability to bind dealers in contracts with third parties as elements of the agency relationship; that can be the *result* of agency, once established.[23]

CDK argues (at 12) that Authenticom "expressly disclaimed" an agency relationship in its contract with dealers, but it acknowledges that legal disclaimers are not controlling. The reality of parties' relationship – rather than the label they attach to it – is determinative. *See Automation by Design*, 463 F.3d at 757; *Oliveira-Brooks v. Re/Max Int'l, Inc.*, 865 N.E.2d 252, 258 (Ill. App. Ct. 2007) ("[T]he declaration of the parties is not controlling where the conduct of the parties demonstrates the existence of an agency relationship."); *Sperl*, 946 N.E.2d at 471 (finding agency relationship despite contract disclaimer).[24] The other provisions of Authenticom's contracts with dealers support an agency relationship. CDK cites (at 13) to § 3.4 of the DealerVault Terms and Conditions, but it omits the pertinent sentence showing the dealer's right to control: "DealerVault shall only extract the Dealership Data that the Dealership permits DealerVault to extract." Dorris Ex. 104 (Dkt. 977-106), at CDK-0012577. The balance of § 3.4 allows Authenticom to set limits

[23] *See 1-800 Contacts*, 722 F.3d at 1250; *ABS Indus., Inc. ex rel. ABS Litig. Tr. v. Fifth Third Bank*, 333 F. App'x 994, 1001-02 (6th Cir. 2009) (rejecting argument that "broad disclaimer of certain fiduciary duties" negated an agency relationship because a "fiduciary relationship" is not a prerequisite for an agency relationship). To the extent Ohio law applies, Ohio follows the Restatement, *see Hensley v. New Albany Co. Ohio Gen. P'ship*, 1997 WL 798776, at *3 (Ohio Ct. App. 1997), which, as explained by *1-800 Contacts* and *ABS Industries*, does not require a showing of a fiduciary relationship or the ability of the agent to bind the principal to establish an agency relationship. *See* Restatement (Second) of Agency § 1 cmt. a (1958) ("The relation of agency is created as the result of conduct by two parties manifesting that one of them is willing for the other to act for him subject to his control, and that the other consents so to act."); Restatement (Third) of Agency § 1.01 cmts. c, d, e (2006). Reynolds's authority – *Eyerman v. Mary Kay Cosmetics, Inc.*, 967 F.2d 213 (6th Cir. 1999) – misapplied the Restatement by treating characteristics of agency relationships (in Sections 12-14) as elements of proof rather than applying the definition of what an agency relationship is (Section 1). *See id.* at 219.

[24] Moreover, CDK's argument rewrites Authenticom's dealer contracts to insert a non-existent comma between "employment" and "agency." At the motion-to-dismiss stage, the Court took no position on CDK's theory that "a comma mistakenly was omitted" between employment and agency, noting that issue "can be fleshed out through discovery." Dkt. 506, at 10-12. But CDK points to no evidence from discovery (because there is none) to support its missing-comma hypothesis. There is thus no factual basis for the Court to rewrite § 10.4, *see* Dorris Ex. 104 (Dkt. 977-106), by inserting a comma where there is none. *See Walker v. Trailer Transit, Inc.*, 824 F.3d 688, 690 (7th Cir. 2016).

– "upon written notice to Dealership," *id.* – with respect to the *dealers' use* of the *DealerVault software*, but that is irrelevant here. As CDK admits (at 17 n.6), the alleged injury-causing conduct is Authenticom's access to the DMS, not the scope of the dealer's right to use the DealerVault platform. Authenticom's boilerplate contract provision allowing it to update the terms of service, *see* Dorris Ex. 104 (Dkt. 977-106), at CDK-0012586, § 10.13, does not defeat the agency relationship either. None of the cases cited by CDK (at 14) remotely supports that proposition.[25]

Finally, CDK (at 15-16) misconstrues the arguments made by counsel for the putative dealership class. The dealership class argued (Dkt. 965, at 70-71) that CDK failed to meet its burden of adducing evidence that the Continental dealership group supervised Authenticom's response to Defendants' CAPTCHA prompts, based in part on CDK's own arguments that Authenticom is not the agent of the dealer. CDK's failure of proof in the dealership case does not speak to whether dealers have the right to control Authenticom's relevant conduct.

II. Summary Judgment Should Be Granted On Defendants' DMCA Counterclaims

As a threshold matter, Authenticom's authorization from dealers to access the DMS negates DMCA liability. *See* Auth. Br. 38. This is because any circumvention must have a nexus to a copyright violation, but there can be no such violation if the access is authorized. *See infra* pp. 53-56 (discussing infringement nexus). Even if this Court held there was no nexus requirement and that Authenticom needed to demonstrate authority to "circumvent" a technological measure in addition to authority to access the work, *see* Reynolds Br. 19-20, Authenticom has done so.

[25] *Daniels v. Corrigan*, 886 N.E.2d 1193 (Ill. App. Ct. 2008), was a fact-specific determination that a cab driver was not an agent of the company that sold him a taxi medallion, based on the substance of the relationship. *Id.* at 1199, 1204-05 (finding lack of right to control based on the substantive relationship). Similarly, *Howland v. BG Products, Inc.*, 2000 WL 1848356 (Wis. Ct. App. 2000) (per curiam), looked to the substance of the relationship and found the alleged principal lacked the right to control any of the details of the agent's work. *Id.* at *5.

Because Authenticom had authority to access the DMS, it necessarily had authority to respond to technological blocking measures that made such access impossible.[26]

Further, to make out a claim under the DMCA – a criminal statute – Defendants must show (1) that Authenticom "circumvented" a technological measure that (2) necessarily protected the copyrighted works and (3) "effectively controlled access" to those works, and (4) a nexus between the circumvention and a copyright violation. Defendants fail to do so.[27]

A. Authenticom Did Not "Circumvent" Any Technological Measures

Defendants' evidence fails to establish that Authenticom "circumvented" any technological measure under the DMCA. Defendants do not dispute that Authenticom accessed their DMSs using valid, dealer-supplied login credentials, which dealers created using built-in DMS functionality that dealers were licensed to use, *see* Auth. Br. 10-11; Resp. ACOM SUF 16-17, 24; that Authenticom responded to CAPTCHA prompts by supplying the text displayed on the screen and to the "Yes/No" prompts by entering "Yes," *see* Auth. Br. 20-21; Resp. ACOM SUF 91, 103; or that Authenticom responded to Defendants' disabling of Authenticom's dealer-supplied credentials by obtaining and using new dealer-supplied credentials, *see* Auth. Br. 21-22; Resp. ACOM SUF 85, 104-106.

[26] Defendants' cases are nothing like this case. They concern situations where a defendant had authority to use a work in one way but defeated a technological measure to use that work in an impermissible way. *See Disney Enters., Inc. v. VidAngel, Inc.*, 869 F.3d 848, 853-54, 863 (9th Cir. 2017) (removed encryption to alter DVD content and play on a different device); *MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 935, 953 n.16 (9th Cir. 2010) (defeating technological measure to use an impermissible cheat with a computer game); *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 436-39, 444 (2d Cir. 2001) (similar to *VidAngel*); *Synopsys, Inc. v. InnoGrit Corp.*, 2019 WL 2617091, at *3 (N.D. Cal. 2019) (circumvented measure to obtain wholly unauthorized access).

[27] Defendants' DMCA claims under 17 U.S.C. § 1201(a)(2) and § 1201(b)(1) fail for the same reasons and for failure to provide evidence of damages. *See* Auth. Br. 41 n.19. Defendants' only reason for treating these claims differently than the § 1201(a)(1) claim is that § 1201(b)(1) explicitly incorporates a copyright nexus requirement. *See* Reynolds Br. 42-43; 17 U.S.C. § 1201(b)(1) (limited to a technological measure "that effectively protects *a right of the copyright owner* under this title in a work") (emphasis added). But this only confirms that Defendants need to prove a copyright nexus, contrary to their arguments that § 1201(a)(1) does not impose such a requirement.

These access means did not violate the DMCA, as a matter of law. The DMCA applies only to acts of circumvention that are the equivalent of removing, disabling, or evading a technological measure, not gaining access to the work by *satisfying* a technological measure by providing the information that the measure requires. The DMCA defines "circumvention" to mean "to descramble a scrambled work, to decrypt an encrypted work, *or otherwise* to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A) (emphasis added). Decrypting and descrambling are ways of removing an access control (the encryption) from a copyrighted work. *See Corley*, 273 F.3d at 452-53 (describing encryption system on DVDs as "like a lock on a homeowner's door, a combination of a safe, or a security device attached to a store's products"). Given the "or otherwise" connector, the generic acts of circumvention – "avoid, bypass, remove, deactivate, or impair" – are naturally read *in pari materia* with "descrambl[ing]" and "decrypt[ing]" as ways of "otherwise" removing or disabling an access control. Indeed, all of the verbs in the definition connote either evading the access control ("avoid, bypass") or disabling it ("remove, deactivate, or impair"). None of these terms reaches a circumstance where access is achieved by satisfying a technological measure in its ordinary operation.

That construction of the DMCA is supported by the statutory definition stating that "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment . . . to gain access to the work." 17 U.S.C. § 1201(a)(3)(B). To "circumvent" – that is, to "avoid, bypass, remove, deactivate, or impair" – such a measure is to defeat the measure by developing a means to access the work *without* applying the "information, or a process or a treatment" that would otherwise be required "in the ordinary course of [the measure's] operation."

The legislative history further demonstrates that Congress enacted the DMCA to criminalize efforts to disable or evade technological measures, not to protect access to copyrighted works more generally. Congress enacted the DMCA to comply with World Intellectual Property Organization ("WIPO") treaties that the United States had joined in 1997. *See Corley*, 273 F.3d at 440. "To comply with the treaties," Congress made it "unlawful to *defeat* technological protections used by copyright owners to protect their works." H.R. Rep. No. 105-551, pt. 1, at 9-10 (1998) (emphasis added). Congress described the prohibited conduct as "the electronic equivalent of breaking into a locked room in order to obtain a copy of a book" – not just obtaining unauthorized access to a book, even by subterfuge. *Id.* at 17.

Defendants have failed to demonstrate that Authenticom engaged in "circumvention" of any of their supposed technological access controls.

1. Login Prompts

It is undisputed that Authenticom responded to login prompts by providing a valid username and password. This Court's prior decision in this case, *see* Dkt. 506, at 16, which followed its earlier decision in *Navistar, Inc. v. New Baltimore Garage, Inc.*, 2012 WL 4338816 (N.D. Ill. 2012) – and the overwhelming weight of authority – holds that the use of valid login credentials is not a DMCA violation, even if the password was obtained without the copyright owner's authorization. *See* Auth. Br. 42-43 & n.21. Responding to a prompt for a login and password with a valid login and password does not evade or disable the prompt; it *satisfies* the prompt through "application of information" required in the ordinary course of operation. 17 U.S.C. § 1201(a)(3)(B); *see Navistar*, 2012 WL 4338816, at *3-4.

Defendants' arguments do not justify departing from the statutory language and these well-reasoned cases. *First*, Defendants' definitions (CDK Br. 32-33; Reynolds Br. 37 & nn.30-31) for the terms "bypass," "impair," and "avoid" *support* the result in *Navistar* and similar cases. As

CDK notes, "bypass" means "to get around"; "impair" means "to diminish" or "to weaken or make worse"; and "avoid" means "to prevent the occurrence or effectiveness of." Satisfying a password prompt with a password does none of those things – any more than using a key to open a lock "bypasses," "impairs," or "avoids" the lock.

Second, Reynolds's cases (at 41-42) holding that using an encryption key is "circumvention" are inapposite. Decryption is unlike the use of valid login credentials because decrypting a work removes the technological measure (the encryption), while providing valid login credentials does not. Reynolds also invokes (at 41) the ejusdem generis canon to argue that the general terms "avoid," "bypass," and "impair" must be interpreted similarly to the specific terms "descramble" and "decrypt." But, as set forth above, *see supra* p. 25, that logic supports Authenticom's interpretation: "avoid," "bypass," "remove," "deactivate," and "impair" should be construed to require disabling a technological measure in the same way that "decryption" and "descrambling" do. There is no suggestion that Authenticom ever defeated the login prompts, as opposed to satisfying them with the requested information.[28]

2. CAPTCHA And Yes/No Prompts

As with satisfying login prompts, responding to CAPTCHA and Yes/No prompts by supplying information that satisfies those prompts is not "circumvention." *See* Auth. Br. 42-44.

a. Reynolds's attempt (at 38) to limit the *Navistar* line of cases to the "narrow" context of login credentials misses the principle underlying those cases – namely, that satisfying a technological measure with the expected information, even if done without authorization, does not

[28] The flaw in the minority of cases holding to the contrary is exemplified by Defendants' principal authority, *Actuate Corp. v. IBM Corp.*, 2010 WL 1340519 (N.D. Cal. 2010). *Actuate* held that the unauthorized use of passwords must be circumvention because there was no basis "in the statute itself for drawing a distinction between passwords and other types of codes that might be used for decryption." *Id.* at *9. But, as explained above, the statute itself makes that distinction in prohibiting "decrypt[ing] an encrypted work . . . without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A).

avoid, bypass, remove, deactivate, or impair those measures. *See, e.g.*, *Navistar*, 2012 WL 4338816, at *5 ("[U]sing a password to access a copyrighted work, even without authorization, does not constitute 'circumvention' under the DMCA because it does not involve descrambling, decrypting, or otherwise avoiding, bypassing, removing, deactivating, or impairing a 'technological measure.' "). *Navistar* itself rejected attempts like Defendants' to cabin this line of cases to the precise "technology at issue." *Id.* ("Whether the focus is on the password or the [password-protected] network, Plaintiffs must adequately allege circumvention . . . .").

Nor does it make any difference whether the intent of Defendants' CAPTCHA and Yes/No prompts was to prevent unauthorized automated access to their DMS. The DMCA does not hinge on the intent behind the technological measure – only on whether there was circumvention. As *Navistar* and other cases correctly hold, use of valid login credentials by unauthorized individuals is not circumvention even though the login prompts are obviously intended to prevent access by those unauthorized individuals. *Navistar* explained:

> [W]hat defendant avoided and bypassed was permission to engage and move through the technological measure from the measure's author. Unlike the CFAA, a cause of action under the DMCA does not accrue upon unauthorized and injurious access *alone*; rather, the DMCA targets the circumvention of digital walls guarding copyrighted material.

2012 WL 4338816, at *4 (quoting *I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004)). Circumvention also does not turn on *how* the information to respond to login prompts (or, here, CAPTCHA prompts) was obtained.[29]

[29] *See, e.g.*, *Digital Drilling Data Sys. LLC v. Petrolink Servs. Inc.*, 2018 WL 2267139, at *14 (S.D. Tex. 2018) (no circumvention for "hacking program" that guessed password), *aff'd*, 965 F.3d 365 (5th Cir. 2020); *I.M.S.*, 307 F. Supp. 2d at 531-33 ("[w]hatever the impropriety of defendant's conduct, the DMCA and the anti-circumvention provision at issue do not target" the unauthorized use of "an otherwise legitimate, owner-issued password"); *Dish Network L.L.C. v. World Cable Inc.*, 893 F. Supp. 2d 452, 464 (E.D.N.Y. 2012) ("[U]sing deception to gain access to copyrighted material is not the type of 'circumvention' that Congress intended to combat in passing the DMCA.").

Reynolds's argument (at 38) misreads this Court's denial of Authenticom's motion to dismiss. This Court accepted as true CDK's allegations that Authenticom engaged in conduct – such as "crack[ing]" the CAPTCHA – that plausibly constituted circumvention. *See* Auth. Br. 43-44. That decision has no bearing now that the summary judgment record shows Authenticom did not evade or disable the measures.

b. Defendants also fail in their attempts to create factual disputes regarding the methods used by Authenticom to respond to CAPTCHA and Yes/No prompts. [redacted]

[redacted]

[30] [redacted]

[31] [redacted]

[redacted]

[redacted] But that distinction cannot transform Authenticom's conduct into "circumvention," because there remains no dispute that Authenticom obtained access to Reynolds's DMS only by accurately providing the information required by the prompt. Even assuming Reynolds's hope was to require information that computers might have a hard time providing, devising a way for a computer to *satisfy* the requirement does not constitute "circumvention." It bears emphasis that Reynolds's [redacted] is not itself a technological measure that can be circumvented under the DMCA, because it does not "require[] the application of information, or a process or a treatment." 17 U.S.C. § 1201(a)(3)(B). And, at any rate, Authenticom never disabled that monitoring system.[32]

[32] The cases that Reynolds cites (at 37-38) do not stand for the proposition that altering one's method of access from a prohibited method (SendKeys) to a permitted method (simulating a physical keyboard) is a DMCA violation. *See Ticketmaster L.L.C. v. Prestige Entm't, Inc.*, 306 F. Supp. 3d 1164, 1174 (C.D. Cal. 2018) (use of methods of access would be "actionable under the DMCA *if used to circumvent* Ticketmaster's technological measures") (emphasis added); *Synopsys*, 2019 WL 2617091, at *3 (generating "counterfeit license keys" through "cracking" files and modifying a computer's identifying information to match those "counterfeit" license keys was "circumvention"); *RealNetworks, Inc. v. Streambox, Inc.*, 2000 WL 127311, at *4, *7 (W.D. Wash. 2000) ("bypassing" an authentication procedure was circumvention).

3. ID Monitoring

The undisputed facts show Authenticom did not "circumvent" Defendants' ID Monitoring.

a. [redacted] Because Authenticom was able to access the DMS without providing *any* information, process, or treatment vis-à-vis ID Monitoring, those measures are not covered by the DMCA. *See* Auth. Br. 54-55; *Auto Inspection Servs., Inc. v. Flint Auto Auction, Inc.*, 2006 WL 3500868, at *8 (E.D. Mich. 2006) (DMCA inapplicable for "user detection feature" that "only comes into play after a user has . . . access[ed] the Program").

[redacted] *Cf. Burroughs Payment Sys., Inc. v. Symco Grp., Inc.*, 2011 WL 13217738, at *4 (N.D. Ga. 2011) ("mere presence of a notice does not 'require[ ] the application of information, or a process or a treatment' ") (alteration in original). CDK (unlike Reynolds) does not claim that its ID Monitoring measure required any information, process, or treatment from the would-be user, instead arguing (at 29-30) that password prompts required a user to supply information. But the password prompt is a separate technological measure that Authenticom did not circumvent. *See supra* pp. 26-27.

Contrary to Reynolds's claim (at 26), Authenticom's argument does not hinge on whether ID Monitoring prohibited initial rather than continuing access. ID Monitoring was not a technological measure because ID Monitoring *never* required any "application of information, or a process or a treatment" to access Reynolds's DMS. 17 U.S.C. § 1201(a)(3)(B). None of Reynolds's cases concerned measures like ID Monitoring that required no information to be provided. *See MDY*, 629 F.3d at 954 (measures required user to "report portions of WoW code running in RAM to the server"); Statement of Material Fact ¶¶ 23-24, *Nexon Am., Inc. v. GameAnarchy, LLC*, No. 12-2083, Dkt. 60 (C.D. Cal. Mar. 18, 2013) (technological measure required users to supply the contents of computer memory for scanning).

That ID Monitoring allowed Authenticom to access the DMS before its login credentials were disabled provides an independent reason why that measure is not covered by the DMCA, which applies only to technological measures that prevent "gain[ing] access to the work," 17 U.S.C. § 1201(a)(3)(B) – not those like ID Monitoring that allow access and then revoke that access at some indeterminate later date. *See* S. Rep. No. 105-190, at 29 (1998) (DMCA "covers protections against unauthorized *initial* access to a copyrighted work") (emphasis added). Reynolds provides no basis to disregard this plain language. The authority on which it relies concerned technological measures that prohibited would-be users from "gain[ing] access," 17 U.S.C. § 1201(a)(3)(B), by persistently scanning for unauthorized access from the start of such access and immediately blocking the access if the measures determined access was unauthorized. *See* Auth. Br. 54-55. [redacted]

b. Even accepting Reynolds's characterization (at 39-40) of Authenticom's efforts to avoid detection by ID Monitoring (which we dispute, ACOM RSUF 39-48), Reynolds at most shows that Authenticom *attempted* to circumvent ID Monitoring. But the DMCA does not prohibit attempted circumvention, *see* Auth. Br. 44-46 – a point that Reynolds does not dispute.

Reynolds has failed to provide evidence that Authenticom *successfully* "circumvented" Reynolds's ID Monitoring. To the contrary, Reynolds has never specified how its ID Monitoring program detected Authenticom's access and disabled its logins or whether Authenticom took steps to "circumvent" the method by which Reynolds was disabling its login credentials. Instead, [redacted]

[redacted][33]

c. Unlike Reynolds, CDK does not argue that Authenticom "circumvented" CDK's disabling of credentials by avoiding detection. CDK instead argues (at 35-36) that Authenticom circumvented CDK's disabling of credentials by re-enabling user credentials through a script called Profile Manager that dealers could use to automate the re-enabling of user credentials. [redacted] This case is thus indistinguishable from *Navistar* and related cases that hold it does not violate the DMCA to use valid login credentials, even if doing so is not authorized by the copyright owner.

CDK tries to avoid that result by contending (at 35) that Profile Manager allowed dealers to re-enable credentials in ways that CDK did not "intend." But, as *Navistar* and similar cases squarely hold, using valid login credentials to access a copyrighted work is not "circumvention" even if an individual uses those credentials without authorization and regardless of any "impropriety" in obtaining those credentials. *Navistar*, 2012 WL 4338816, at *5. Further, CDK's claim (at 35) that it "expressly sought to prevent" dealers from re-enabling login credentials is unsupported by any evidence and thus cannot defeat summary judgment. CDK provides no evidence that it ever implemented any measure to limit a dealer's ability to re-enable login

[33] Reynolds's assertion (at 40) that its damages expert has "painstaking[ly]" counted the number of times that Authenticom "circumvented" Reynolds's ID Monitoring is incorrect. [redacted]

credentials either manually or automatically during the period that it claims Authenticom used Profile Manager for circumvention. *See* Resp. ACOM SUF 106. Indeed, on April 25, 2017, CDK implemented a new technology measure to prohibit Profile Manager from re-enabling login credentials. *See id.* CDK does not claim that Authenticom ever "circumvented" this technology measure once put into place. [redacted]).[34]

* * *

Defendants also resort to scattered statements by Authenticom employees as evidence that it engaged in "circumvention." *See* CDK Br. 33-34; Reynolds Br. 35. But Authenticom employees did not believe their access was unauthorized or that they were violating any laws; nor did CDK employees when they used the same methods to access Reynolds's DMS. *See* Auth. Br. 14-15; ACOM SUF 28, 51-52. In any event, the words that Authenticom employees used to describe their methods of access are at best inadmissible legal conclusions. *See United States v. Noel*, 581 F.3d 490, 496 (7th Cir. 2009) ("lay testimony offering a legal conclusion is inadmissible"); *Chubb Indem. Ins. Co. v. 21 E. Cedar, LLC*, 2014 WL 2619469, at *5 (N.D. Ill. 2014) ("[L]ay witness testimony that an act was negligent [does not] make[ ] it legally so.").[35]

[34] For the reasons given in Authenticom's opening brief (at 45-46) and in the Dealers' briefing (arguments that Authenticom incorporates by reference), this Court should reject CDK's attempt to inflate statutory damages by counting each time that Profile Manager ran on a dealer's computer as a DMCA violation regardless of whether Profile Manager re-enabled an account.

[35] [redacted]

B. The Technological Measures Did Not Protect Copyrighted Works

Defendants' DMCA claims fail because Defendants have failed to present any evidence that their purported technological measures "protected" any copyrighted works. *See* Auth. Br. 46-49. Defendants assert their technological measures "protected" three copyrighted works: (1) the "client" software (consisting of executable code and screen displays), (2) the "server" software, and (3) the information displayed through the "client" software (the "data compilations"). *See* Reynolds Br. 27; CDK Br. 41-42.[36] Defendants' purported showing in this regard fails at the outset, however, because Defendants rely on declarations that are improper under Rule 37. Further, whether or not those declarations are considered, Defendants' arguments fail because (1) as to the "client" software, the evidence is undisputed that Authenticom could access that executable code without encountering technological measures, and Defendants have also failed to show that the "screen displays" were copyrightable; (2) Authenticom never accessed the server software; and (3) any information displayed via "client" software (the "data compilations") was not protected by any technological measure because, as Defendants have admitted, Authenticom could obtain the same data compilations by other means without encountering any blocking.

1. Defendants' Declarations Should Be Excluded

Defendants' arguments all depend not on evidence developed during discovery but instead, in CDK's case, on two declarations from Northon Rodrigues dated May 18, 2020, and July 27, 2020, *see* Fenske Ex. 108 (Dkt. 975-108) and Fenske Ex. 523 (Dkt. 1065-55) (cited at CDK Br.

[36] Authenticom's opening brief focused on the "client" software – both the executable code and the visual displays – because that is the only software accessed by Authenticom. *See* Auth. Br. 46-49. CDK asserts (at 39 n.15) that its counterclaims were based on "copyrightable aspects" of CDK's client software that were not addressed by Authenticom's motion for summary judgment. But the allegation cited by CDK states "CDK's terminal program" – the client software – "is an original and independent work" consisting of "source and object code; distinctive screen layouts; graphical content; text; arrangement, organization, and display of information." Dkt. 229, CDK Counterclaims ¶ 21. Authenticom addressed each of those aspects – the code itself and the visual displays. *See* Auth. Br. 46-49.

38-40; DJ SUF 20-21; DJ SAF 53-54), and in Reynolds's case on two declarations from Kelly Hall dated May 19, 2020, and July 27, 2020, *see* Fenske Ex. 107 (Dkt. 975-107) and Fenske Ex. 524 (Dkt. 1065-56) (cited at Reynolds Br. 27-30; DJ SUF 3; DJ SAF 55-66). These declarations should be excluded pursuant to Rule 37, which mandates exclusion of evidence where "a party fails to provide information or identify a witness as required by Rule 26(a) or (e) . . . unless the failure was substantially justified or is harmless." Fed. R. Civ. P. 37(c)(1). *See Tribble v. Evangelides*, 670 F.3d 753, 760 (7th Cir. 2012).

First, CDK never disclosed its declarant (Northon Rodrigues) as an "individual likely to have discoverable information." Fed. R. Civ. P. 26(a)(1)(A)(i); *see* Ho Ex. 515, CDK's Am. and Suppl. Rule 26(a)(1) Initial Disclosures (Apr. 30, 2019). CDK makes no attempt to justify its reliance on an undisclosed witness to supply evidence on a necessary element of its DMCA claims for which it asserts hundreds of millions of dollars in damages. The prejudice is plain, because it deprived Authenticom of the opportunity to subject the evidence to discovery and expert analysis. *See Bamcor LLC v. Jupiter Aluminum Corp.*, 767 F. Supp. 2d 959, 970 (N.D. Ind. 2011). The declaration must be excluded. *See Steffek v. Client Servs., Inc.*, 948 F.3d 761, 768 (7th Cir. 2020) ("[A] motion for summary judgment supported by an affidavit from a witness not previously disclosed in the case ordinarily will cause problems that Rule 26(a)(1)(A)(i) and (e)(1) and case management plans are intended to prevent."); *accord, e.g.*, *Rice ex rel. Rice v. Corr. Med. Servs.*, 675 F.3d 650, 669 (7th Cir. 2012) (excluding summary judgment affidavits); *Sanchez v. Garcia*, 2015 WL 2097606, at *3 n.5 (N.D. Ill. 2015) (same).[37]

[37] In addition to failing to disclose Rodrigues as a witness with discoverable information, his name does not appear in CDK's document production. According to his LinkedIn profile, Rodrigues began working at CDK only in January 2018 – generally after the dates of documents produced in this MDL – and after Authenticom's alleged circumvention of technological measures. Thus, it appears Rodrigues may have no personal knowledge about the technological measures during the relevant time period.

Second, Defendants seek to rely on declarations describing how their technological measures function (and what they protect) even though Defendants refused to provide discovery on that same issue. Authenticom specifically sought – and moved to compel production of – "system design documents" (Dkt. 318, at 25-27), including those relating to "blocking automated access to data on your DMS." *See* Ho Ex. 513, Auth. RFP to CDK No. 74; Ho Ex. 514, Auth. RFP to Reynolds No. 64.[38] Defendants conceded these documents would be relevant to "circumvention of their DMS security measures" but opposed that discovery on grounds that it would be burdensome to "search[ ] through and produc[e] documents from the files of engineers, programmers, or other technical personnel," and such materials would not be relevant and are sensitive. Dkt. 354, at 29-30. Judge Gilbert denied Authenticom's motion to compel. *See* Dkt. 441, at 8. Having successfully opposed discovery of how their technological measures worked, Defendants cannot now rely on declarations addressing the same subject matter.[39]

Without these declarations, Defendants have no evidence to support their claims that their technological measures protected copyrighted works. The *only* other evidence cited by CDK is a single screenshot from a video used by Authenticom's expert Nancy Miracle to demonstrate the operation of Authenticom's data integration service. *See* DJ SAF 54 (citing Fenske Ex. 15, at .0032). That screenshot does not meet their burden. *See infra* pp. 42-44. And the *only* evidence

[38] *See also* Ho Ex. 513, Auth. RFP to CDK No. 79 ("All documents and communications relating to the technological methods used by CDK to block or disable dealer-provided login credentials."); Ho Ex. 514, Auth. RFP to Reynolds No. 69 (same).

[39] *See Hardin v. Dadlani*, 221 F. Supp. 3d 87, 104 (D.D.C. 2016) ("[P]ursuant to [Rule] 37(c), the Court found that it was necessary to preclude information specifically requested by the plaintiff during discovery but that the defendant failed or otherwise refused to produce."); *Hooks v. Forman Holt Eliades & Ravin LLC*, 2015 WL 5333513, at *6 (S.D.N.Y. 2015) (striking summary judgment declaration because "Defendant cannot, on the one hand, refuse to produce [a document] because it is 'not relevant to any parties' claims or defenses' . . . and on the other, assert facts characterizing [that document]"); *Norbrook Labs. Ltd. v. G.C. Hanford Mfg. Co.*, 297 F. Supp. 2d 463, 481 (N.D.N.Y. 2003) (striking testimony for failure to produce requested documents on the same subject matter), *aff'd*, 126 F. App'x 507 (2d Cir. 2005).

cited by Reynolds other than the Hall declarations are four lines of a deposition stating that "different DMSs have different data fields." *See* DJ SUF 3; Fenske Ex. 328 (Dkt. 979-128), Lamb Tr. 187:9-12. That statement has nothing to do with Reynolds's technological measures, whether those measures protect any works, or whether such works are copyrightable.

In any event, whether or not these declarations are considered, Defendants fail to present evidence to satisfy this element of their claims.

2. Defendants Present No Evidence That The Technological Measures Protected Access To Their Client Software

a. Defendants fail to present evidence that the technological measures at issue protected their client software because it is undisputed that Authenticom can access the entirety of the executable code for their client software without encountering any technological measures. This is fatal to Defendants' DMCA claims, because, if one can access a copyrighted work without encountering the technological measure, the measure cannot be said to "protect" the work. "Just as one would not say that a lock on the back door of a house 'controls access' to a house whose front door does not contain a lock . . . , it does not make sense to say that this provision of the DMCA applies to otherwise-readily-accessibly copyrighted works." *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 547 (6th Cir. 2004).

The Fifth, Sixth, and Ninth Circuits unanimously recognize this requirement. *See* Auth. Br. 46-49. In *Lexmark*, for example, Lexmark implemented "an 'authentication sequence' that performs a 'secret handshake' " to ensure that only authorized printer cartridges were used with its printers. 387 F.3d at 530. A competitor (SMARTEK) sold printer cartridges that were not authorized by Lexmark and "boast[ed] that its chips break Lexmark's 'secret code' (the authentication sequence)," and, to make those chips work, SMARTEK "slavishly copied" Lexmark's Toner Loading Program software. *Id.* at 530-31. Lexmark contended that SMARTEK violated the DMCA by circumventing the "authentication sequence" to access Lexmark's printer software. *See id.* at 546. But despite the fact SMARTEK concededly "br[oke]" that "secret code," *id.* at 530, the Sixth Circuit held there was no DMCA violation because one could access the software without encountering the technological measure: "Anyone who buys a Lexmark printer may read the literal code of the Printer Engine Program directly from the printer memory, with or without the benefit of the authentication sequence." *Id.* at 546; *see MDY*, 629 F.3d at 952 (same).

Similarly, in *Digital Drilling Data Systems, L.L.C. v. Petrolink Services, Inc.*, 965 F.3d 365 (5th Cir. 2020), a software company (Digital Drilling) sought to protect its proprietary software by designing it "to run only when a USB security dongle is plugged into the laptop." *Id.* at 370. A competitor (Petrolink) began to use output from Digital Drilling's software to provide service to its own customers without paying Digital Drilling. *See id.* at 371. Petrolink did so by finding a way to access a Digital Drilling database without use of the "USB security dongle" and through a program "dubbed 'the scraper' or 'the hack.'" *Id.* Despite Digital Drilling's clear intent to implement a technological measure to prevent unauthorized access – and the use of a "hack" – the Fifth Circuit held there was no DMCA violation because Petrolink had devised methods to access the database "without ever encountering th[e] [technological] measures." *Id.* at 376.

b. That principle bars Defendants' claims with respect to their "client" software that dealers (and their agents) employ to use the DMS. [redacted]-

[redacted]

c. For the visual elements displayed through the client software, Defendants have failed to carry their burden of presenting evidence that any such elements accessed by Authenticom were protected by technological measures and copyrightable. *See* Auth. Br. 47-49.

Reynolds. Reynolds asserts (at 27-28) that its registered copyrights in its executable programs extend not only to the code but also to the screen displays. *See* RSUF 5 (citing copyrights

[40] Whether Authenticom could have accessed Reynolds's source code, *see* DJ SAF 60, is irrelevant because there is no suggestion that Authenticom accessed Reynolds's source code. *See Corley*, 273 F.3d at 438-39 (explaining difference between executable and source code).

for the executable programs ERAccess.exe and ERA-Ignite.exe). This undercuts Reynolds's DMCA claim. The Library of Congress has explained that a registered copyright for software covers the "computer program code and screen displays" because both "are integrally related and ordinarily form a single work." Registration and Deposit of Computer Screen Displays, 53 Fed. Reg. 21,817, 21,819 (June 10, 1988). [redacted]

MDY is squarely on point. As here, there was no technological measure that prohibited access to the "client's software code," which was "available on [the user's] hard drive" or that prohibited access to "the visual images or the recorded sounds" generated by the "client's software." 629 F.3d at 952; *see also Lexmark*, 387 F.3d at 546-47 (DMCA claim failed due to capability to "read the literal code . . . directly from the printer memory"). [redacted]

CDK. [redacted]

[redacted]

[redacted] This threadbare showing is insufficient to support CDK's claims to hundreds of millions of dollars of damages. Among other things, CDK never provides evidence of which screen displays Authenticom accessed and whether it would have encountered any technological measure (and which one) before accessing those screens. [redacted]

[redacted] CDK's screen display is indistinguishable from the one rejected in *Avaya, Inc. v. Telecom Labs, Inc.*, 2012 WL 13035096 (D.N.J. 2012). There, the court dismissed a DMCA claim based on "screen displays [that] are the product of technical constraints and functional considerations, not original, aesthetic-minded choices," and whose "short phrases, typographical ornamentation, and minimal coloration lack originality, and thus are not protectable by copyright." *Id.* at *8-9; *see id.* at *8 (citing Copyright Office guidance that "menu screens and similar functional interfaces consisting of words or brief phrases in a particular format are not registrable"). That opinion even includes a screenshot that is almost exactly the same CDK's screenshots. CDK makes no attempt to address this case, which was relied on in Authenticom's motion. *See* Auth. Br. 47-49; *see Real View, LLC v. 20-20 Techs, Inc.*, 683 F. Supp. 2d 147, 154, 158-66 (D. Mass. 2010) (analyzing copyrightability of screen displays).[41]

3. Authenticom Never Circumvented Any Technological Measure To Access (And Never Did Access) Defendants' Server Software

Defendants' DMCA claims with respect to their server software fail because Authenticom never accessed that software through circumvention or otherwise. [redacted]

[redacted]

[41] Defendants raise several legal disputes that are ultimately immaterial due to the lack of any evidence to support their claims. *First*, Authenticom relies on Defendants' inability to show originality and creativity – for which Defendants bear the burden – in addition to *scenes a faire*. *See* Auth. Br. 49-51. *Second*, even if Authenticom did rely solely on *scenes a faire*, the better reasoned decisions hold that this goes to copyrightability (as to which Defendants carry the burden), and, even if *scenes a fair* were an affirmative defense, Defendants have shown no prejudice from its consideration. *See Lexmark*, 387 F.3d at 535. *Third*, even though copyrightability is generally a question to be resolved by a court in the Seventh Circuit (but not other circuits), expert evidence is still relevant and necessary in complicated software cases like this. *See Team Play, Inc. v. Boyer*, 391 F. Supp. 2d 695, 699-700 (N.D. Ill. 2005); *Francescatti v. Germanotta*, 2014 WL 2767231, at *8-11 (N.D. Ill. 2014).

[redacted]

Defendants thus are left to argue that Authenticom "accessed" the server software because the client software used by Authenticom communicated with Defendants' server software. [redacted] This is not "access" within the meaning of the DMCA. "Because Congress did not explain what it means to 'gain access to the work,'" this Court should apply the ordinary meaning of "access": "'the ability to enter, to obtain, or to make use of.'" *Lexmark*, 387 F.3d at 546 (quoting *Merriam-Webster's Collegiate Dictionary* 6 (10th ed. 1999)). Authenticom plainly did not "enter" or "obtain" the server software. Nor did Authenticom "make use of" that software. Authenticom indisputably used the client software (as a dealer employee would), and that client software "made use of" the server software. Defendants cite no case supporting a construction of the DMCA that covers such *indirect access* to copyrighted works, and Authenticom is aware of none. This Court should not be the first to adopt such a broad construction of the DMCA (a criminal statute), contrary to the rule of lenity. *See* Auth. Br. 37 (citing *United States v. Valle*, 807 F.3d 508, 523 (2d Cir. 2015)).

Furthermore, even if the DMCA covered indirect access, there would be no DMCA violation for accessing Defendants' server software. It is undisputed that Authenticom never obtained a copy of the server software; *Defendants* copy that software into memory on *Defendants'* servers. [redacted] In related litigation, Judge Snow of the District of Arizona correctly held that causing the copyright owner to create copies of its own programs in its own servers is not a copyright violation. *See CDK Glob. LLC v. Brnovich*, 2020 WL 4260506, at *2-3 (D. Ariz. 2020). The same is true here.[42]

4. There Is No DMCA Violation With Respect To Defendants' Data Compilations Because They Allowed Authenticom To Obtain Those Data Compilations By Manual Means

Defendants concede that Authenticom could obtain the "data compilations" in the same format as long as dealer employees exported the reports and provided them to Authenticom. *See* Reynolds Br. 29 n.21 ("Reynolds's license agreements and policy permit authorized dealership employees to send exported data reports to third parties of their choice."); Dkt. 966, at 5 ("[B]oth DMSs have built-in reporting tools allowing dealers to export (or 'push') data to a file that can be

[42] In that litigation, Defendants here (but plaintiffs there) had contended (based on a declaration from Kelly Hall, also Reynolds's declarant here) that "automated access . . . results in the unauthorized use and copying of Plaintiffs' copyrighted DMS software." 2020 WL 4260506, at *2. But discovery disproved that contention: the "server software" is "run by Reynolds on Reynolds' own servers." *Id.* at *2 n.8. The fact that evidence developed during discovery disproved Defendants' similar contentions in related litigation highlights the prejudice caused by Defendants' refusal to provide discovery into these matters. *See supra* pp. 36-39.

sent to vendors without any third-party access to the DMS."). That is fatal under the DMCA. Because Authenticom could and did obtain the "data compilations" without encountering any technological measures, Defendants' technological measures did not protect those works. *See* DJ SUF 39.

C. Defendants' Technological Measures Did Not "Effectively Control Access"

The DMCA applies only to technological measures that "effectively control access," which means that they be capable of distinguishing between authorized and unauthorized users. *See* Auth. Br. 49-51. There is no genuine dispute that Defendants' technological measures have no such capability. Those measures either display to all potential users the information needed to proceed (CAPTCHA and Yes/No prompts) or do not even require a potential user to provide any information (ID Monitoring). *See* Auth. Br. 51-54.[43] [redacted][44]

1. Defendants instead contend that any technological measure that "require[s] the application of information, or a process or [a] treatment . . . to gain access to the work" – no matter how simplistic – is covered by the DMCA. Reynolds Br. 21; CDK Br. 29-30. For example, Reynolds claims (at 21) that a prompt with instructions requires both application of a process

[43] [redacted]

[44] [redacted]

(reading) and information (following the instructions), and is thus a technological measure covered by the DMCA. And CDK argues (at 29) that a prompt requiring the user to type "YES" is a technological measure that "effectively controls access" within the meaning of the DMCA.

Defendants' overbroad interpretation is contrary to the statutory text and the legislative history, and it is inconsistent with how access controls are understood within the computer security industry. Textually, a measure "effectively controls access" to a work only if in its ordinary operation it "requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." The phrase "with the authority of the copyright owner" modifies the preceding phrase "application of information, or a process or a treatment" – that is, the "information," "process," or "treatment" must be one that can differentiate between authorized and unauthorized users and permit access to authorized but not unauthorized users. That is, of course, the natural meaning of an effective access control: a technological measure that limits access to those who have "authority of the copyright owner."[45]

Defendants' competing interpretation is that the phrase "with the authority of the copyright owner" means only that the "measure must be one put in place by the copyright owner." Reynolds Br. 22; CDK Br. 29, 31. That is not what the statute says. The clause "with the authority of the copyright owner" refers to the functionality of the technological measure, not *who* must implement the measure. 17 U.S.C. § 1201(a)(3)(B). Indeed, because it is difficult to imagine circumstances in which a technological measure would be "put in place" by someone other than the copyright

[45] Defendants misplace reliance on cases interpreting the clause "without the authority of the copyright owner" in the context of § 1201(a)(3)(A). *See* Reynolds Br. 22-23. There, the clause modifies the acts that the DMCA defines to be "circumvent[ion]" – to "descramble," "decrypt," "avoid," "bypass," "remove," "deactivate," or "impair." The statute thus prohibits those acts of circumvention when performed "without the authority of the copyright owner." *See Disney Enters.*, 869 F.3d at 863; *MDY*, 629 F.3d at 953 n.16; *Corley*, 273 F.3d at 444 & n.15. But the relevant provision here is § 1201(a)(3)(B) in which a similar clause modifies what the technological measure must "require."

owner, Defendants' counter-textual interpretation would effectively nullify the phrase "with the authority of the copyright owner."

The legislative history (which Defendants do not address) also forecloses their interpretation. Congress explained that "a technological measure effectively controls access" within the meaning of § 1201(a)(3)(B) only when they are "'based on encryption, scrambling, authentication, or some other measure which requires the use of a "key" provided by a copyright owner to gain access to a work.'" Auth. Br. 49-50 (quoting H.R. Rep. No. 105-551, pt. 2, at 39 (1998)). That is, the measure must "require" a "key" that demonstrates "authority."

Congress's definition of "access control" in the DMCA also tracks the accepted definition of that term in the computer security field. *See id.* at 50-51 (quoting *Corning Glass Works v. Brennan*, 417 U.S. 188, 201 (1974) (it is "proper to explain [technical words or terms of art] by reference to the art or science to which" they are "appropriate")). Reynolds cites a National Institute of Standards and Technology ("NIST") definition for "access control" as "the process of permitting or restricting access to applications at a granular level such as per user, per group and per resources." Reynolds Br. 25 (emphasis omitted).[46] This definition confirms that determining a user's authorization is a necessary component of an access control: "[t]he process of permitting or restricting access . . . per-user, per-group, and per-resources" requires identification of the would-be user and determining what authorization that would-be user has. NIST Publ'n at A-1;

[46] Reynolds plucks this definition from NIST's glossary of terms that lists the various ways in which terms are used in different NIST publications. For "access control," there are 16 definitions provided by NIST from 16 different publications. *See* https://csrc.nist.gov/glossary/term/access_control. The one that Reynolds chooses to highlight comes from NIST Special Publication 800-113, *Guide to SSL VPNs* (July 2008) ("NIST Publ'n"). This publication explains: "Access privileges may be granted to individuals, groups, or resources. For ease of configuration, access control is typically configured based on groups. Each user is assigned to one or more groups, each group having certain security parameters. Group information may be accessed from the authentication database, such as the LDAP directory. Access control may also be defined for a set of resources instead of an individual resource." *Id.* at 3-7.

see id. at 3-3 ("Authentication is the process a VPN uses to limit access to protected services by forcing users to identify themselves."). Other NIST definitions that Reynolds does not mention make even more explicit that determining a would-be user's authorization is a necessary component of an access control. *See*, *e.g.*, https://csrc.nist.gov/glossary/term/access_control (defining "access control" as the "[p]rocess of granting access to information system resources only to authorized users, programs, processes, or other systems").

Fundamentally, Defendants' proposed interpretation would lead to the absurd result that every interactive element of software (such as a click button, menu, or text box) "put in place" by the creator of the software is a technological measure covered by the DMCA because those elements "require" the "application of information, or a process or a treatment." Defendants' interpretation would thus make it a federal crime, *see* 17 U.S.C. § 1204, to interact with those software elements without authorization from the copyright owner. [redacted] Congress did not create the DMCA to criminalize virtually every use of software when done "without the authority of the copyright owner." As the Second Circuit has explained, the DMCA protects only "the efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections." *Corley*, 273 F.3d at 435.

Defendants' authority does not compel their overbroad reading of the statute. They note that this Court previously ruled CDK had plausibly alleged "circumvention," but that decision did not address whether any of Defendants' technological measures effectively controlled access to a protected work within the meaning of the DMCA. *See* Dkt. 506, at 17-18. They also rely on a series of district court decisions holding that claims asserting DMCA protection for CAPTCHA are plausible. *See* Reynolds Br. 21 & n.14. This line of decisions stems from a single case – *Ticketmaster L.L.C. v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096 (C.D. Cal. 2007) – with scant independent analysis in each subsequent decision. Further, each of these decisions was made prior to any factual development.[47] These decisions are not binding on this Court and need not be followed when the factual record in this case shows that Defendants' technological measures had no capability to distinguish authorized from unauthorized users.[48]

Finally, Reynolds incorrectly asserts (at 23-24) that – in addition to the CAPTCHA cases (which should not be followed for the reasons above) – courts routinely hold that technological measures are covered by the DMCA even though those measures are incapable of determining whether a user has authorization from the copyright owner. Each of Reynolds's examples – password prompts and encryption schemes (CSS) – *do* attempt to determine whether a user is authorized. Those measures require the prospective user to provide a "key" (a login password or encryption key) to gain access to the work, and, because those "keys" are given only to authorized users, the usage of the "key" indicates authorization. To be sure, those methods are not foolproof because an unauthorized user might obtain the "key" or develop other means to bypass the measure without supplying the "key." But, unlike here, those measures have the crucial feature of having some ability to distinguish between authorized and unauthorized users. *See MDY*, 629 F.3d at 954

[47] *See RMG*, 507 F. Supp. 2d at 1111-12 (preliminary injunction decided based on written submissions); *Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1056 (N.D. Cal. 2010) (following *RMG* on a motion to dismiss); *Craigslist, Inc. v. Kerbel*, 2012 WL 3166798, at *9-10 (N.D. Cal. 2012) (following *Naturemarket* and *RMG* on a motion for default judgment); *Prestige Entm't*, 306 F. Supp. 3d at 1174 (motion to dismiss); *Ticketmaster L.L.C. v. Prestige Entm't W., Inc.*, 315 F. Supp. 3d 1147, 1166-67 (C.D. Cal. 2018) (following *RMG* and *Kerbel* on a motion to dismiss).

[48] To the extent those decisions purport to hold that all CAPTCHA (and similar prompts) are access controls covered by the DMCA, they were wrongly decided.

n.17 (citing *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001)).

2. Finally, Reynolds incorrectly asserts (at 20-21) that its technological measures must be assessed collectively. The DMCA requires separate consideration of whether each technological measure effectively controls access and whether that technological measure has been circumvented. *See* 17 U.S.C. § 1201(a)(1)(A), (a)(3). Each relevant section refers to "a technological measure" (singular) – not a combination of technological measures. *See id.* Indeed, Defendants treat their technological measures as distinct for purposes of the DMCA and claim separate damages for each alleged circumvention of the different technological measures. *See* Dkt. 785, at 9-16 (Reynolds treating CAPTCHA and ID Monitoring as distinct measures); Auth. Br. 60-61; Dorris Ex. 147 (Dkt. 977-149), Rubinfeld CDK Rep. ¶¶ 77-79 & Tbl. 5 (CDK asserting separate statutory damages for alleged circumvention of CAPTCHA, Yes/No prompts, and ID Monitoring). They cannot have their cake and eat it too.

Even the cases on which Defendants rely do not combine separate technological measures to meet the DMCA's requirements. *MDY* considered two components of the same technological measure – one that did an initial scan at login and another that continued the scan throughout use of the program – but Defendants seek cumulative treatment of different measures. *See* 629 F.3d at 943. And, even then, *MDY* considered separately whether these components of the same measure effectively controlled access. *See id.* at 954. The other case cited by Reynolds – *RealNetworks, Inc. v. Streambox, Inc.*, 2000 WL 127311 (W.D. Wash. 2000) – also separately discussed whether each of the two measures was covered by the DMCA. *See id.* at *7.

In any event, cumulative treatment of Defendants' technological measures changes nothing. It is undisputed that *none* of Defendants' measures – except the password prompt, which

Authenticom never circumvented – had any capability to determine whether a prospective user was authorized to access the DMS. The same remains true when they are combined together: "zero plus zero still equals zero." *Ray v. Clements*, 700 F.3d 993, 1017 (7th Cir. 2012).

D. Defendants Cannot Establish A Nexus To A Copyright Violation

As district courts in this Circuit and the Federal Circuit have held, the DMCA requires that any act of circumvention have a nexus to a subsequent copyright violation. Here, the only purported copyright violation identified by Defendants is Authenticom's unauthorized use of their DMS software. But Authenticom used their DMS software only as an intermediate (and transitory) step to obtain access to data stored on the DMS in which Defendants had no proprietary or copyright interest. Under *Assessment Technologies of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640 (7th Cir. 2003), that was fair use. *See* Auth. Br. 55-60.

1. The DMCA Imposes An Infringement Nexus

Defendants urge this Court to reject the unanimous holdings of district courts in this Circuit and of the Federal Circuit that the DMCA requires a nexus between "circumvention" and a copyright violation. None of Defendants' reasons for rejecting these cases has merit.

First, Reynolds claims (at 43-44) that *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F.3d 1178 (Fed. Cir. 2004), is "irrelevant" because Defendants have sought to limit third-party DMS access by contract. But Defendants over-read the footnote on which they rely. There, the Federal Circuit merely noted that there was no argument that the copyright owner had imposed any such contractual limitation on consumers, and it thus "d[id] not reach" the issue whether the DMCA would apply where the would-be user voluntarily agreed not to access a work and where the technological measure protects such contract limitations rather than rights under the Copyright Act. *Id.* at 1202 n.17. That footnote does not apply here because *Authenticom* never voluntarily agreed not to access Reynolds's DMS. Thus, as to Authenticom, the technological measure was not protecting contractual limitations.

Second, Reynolds tries (at 45) to avoid the clear import of 17 U.S.C. § 1201(c)(1) in claiming that this provision "does not change the scope of Section 1201(a)." Section 1201(c) does limit the reach of § 1201(a) by providing that "[n]othing in *this section* shall affect rights, remedies, limitations, *or defenses* to copyright infringement, *including fair use*." 17 U.S.C. § 1201(c)(1) (emphases added). That provision squarely retains the fair use defense to any purported DMCA violation. As *Chamberlain* explained, the DMCA cannot be construed to allow a copyright owner to employ technological measures to restrict access to copyrighted works where the subsequent use would be fair use because such a construction would necessarily "affect" the defense of fair use. 381 F.3d at 1199-1201. Indeed, even *MDY* – Defendants' preferred authority – did not hold that fair use was not a defense to DMCA liability; nor could it, given the express statutory provision retaining that defense. *See* 629 F.3d at 950 n.12 ("[W]e too leave open the question whether fair use might serve as an affirmative defense to a prima facie violation of § 1201.").[49]

Third, Reynolds repeats (at 44-45) the flawed reasoning of *MDY* that rests on the difference in language between § 1201(a)(2) – which addresses circumvention of "a technological measure that effective controls access to" a copyrighted work – and § 1201(b) – which addresses circumvention of "a technological measure that effectively protects a right of a copyright owner." The difference in language exists because Congress created separate provisions to address different types of circumvention devices: § 1201(a)(2) addresses devices that restrict *access* (such as a

[49] *Chamberlain* left open the question whether fair use would be a defense to DMCA liability where circumvention enabled *others* to use the copyrighted work in ways that would be fair use. *See* 381 F.3d at 1199 n.14. The Court need not reach that question because Authenticom's alleged circumvention was in furtherance of its *own* fair use. Similarly, Defendants misplace reliance on *Corley*. There, the defendant did not claim that it was entitled to a fair use defense. It claimed a fair use defense only because its anti-circumvention devices may have enabled fair use by *others*. *See* 273 F.3d at 443-44.

password prompt), and § 1201(b) addresses devices that restrict *copying* (such as digital watermarking methods that prohibit copies of a work). *See* Auth. Br. 57-58 (citing legislative history); *RealNetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 938 (N.D. Cal. 2009) (explaining separate operation of these provisions). There is thus no basis to infer from the difference in the text that the DMCA abrogates fair use defenses, especially given the explicit savings clause for the fair use defense in § 1201(c)(1).

Fourth, Reynolds incorrectly claims (at 44-45) that recognizing a fair use defense would render superfluous the DMCA provisions permitting the Librarian of Congress to exempt certain classes of users and works. *See* 17 U.S.C. § 1201(a)(1)(B)-(E). That exemption authority allows the Librarian to provide explicit guidance that the DMCA does not apply to certain noninfringing uses without individuals needing to establish a fair use defense in each individual case and without the uncertainty that the factfinder might reject such a defense. But that exemption authority exists in addition to (not to the exclusion of) the traditional fair use defense that the DMCA preserves in § 1201(c)(1). Indeed, the Librarian's authority may be exercised only once every three years, *see id.* § 1201(a)(1)(C), which indicates that such authority does not supplant fair use rights.

Fifth, Reynolds asserts (at 45) that imposing an infringement nexus would render the entire DMCA superfluous because any DMCA violation would already be a copyright violation. That is not correct: the DMCA prohibits discrete conduct not addressed in the Copyright Act – including both circumvention and trafficking in circumvention devices, *see* 17 U.S.C. § 1201(a)(2), (b) – and imposes additional remedies, *see id.* §§ 1203, 1204.

Sixth, Defendants' principal authority, *MDY*, by its own terms does not apply to this case. *MDY* distinguished the Federal Circuit's *Chamberlain* decision by explaining that the concern that the DMCA "would allow companies to leverage their sales into aftermarket monopolies, in potential violation of antitrust law and the doctrine of copyright misuse," was not a concern in *MDY*. 629 F.3d at 949, 951. The Ninth Circuit noted that its opinion would not control in "a future case" – like this one – where "a plaintiff is attempting to enforce its DMCA anti-circumvention right in a manner that violates antitrust law." *Id.* at 951; *see* Dkt. 1081, at 7-11.

2. Authenticom's Use Of DMS Software Was Fair Use

Binding Seventh Circuit authority in *WIREdata* compels summary judgment in favor of Authenticom on its fair use defense. *See* Auth. Br. 58-60. Defendants' principal argument is that nearly three-quarters of *WIREdata* is dicta. *See* Reynolds Br. 47. Not so. As an initial matter, the facts of the case are very similar to the facts of this case, and, thus, *WIREdata* controls the result here. In *WIREdata* – as here – a database owner stored data in a proprietary database; the database owner at most had a copyright interest in the formatting of the data within the database; and the database owner had no copyright interest in the raw data. *See* 350 F.3d at 642-44. And, as here, the accused infringer sought access to the raw data, which could be accomplished only by extracting the raw data from the database owner's proprietary database. *See id.* at 643-44. The Seventh Circuit held that, regardless of how the data was extracted, there was no copyright violation because there was copying of only the non-copyrightable raw data, not the copyrightable proprietary database. *See id.* at 644. That same ruling applies here because – regardless of how Authenticom extracts data from Defendants' DMS – there is no evidence that Authenticom copies the DMS or the format in which the data is stored in the DMS. *See* ACOM SUF 26 (Authenticom accesses a subset of data authorized by dealers).

The Seventh Circuit further explained that, even if the extraction process required intermediate copying of Defendants' proprietary database software (Market Drive) to extract the data, such copying would be fair use. *See WIREdata*, 350 F.3d at 644-45. That portion of the Court's opinion was not dicta because the database owner had argued that it would be a copyright violation to extract the data. *See* Appellee Br. 24, 2003 WL 22721369. The Seventh Circuit rejected this argument for two independent reasons – first, there would be no copyright violation because only raw data would be copied; second, even if the database owner's software or format was copied, such copying would be fair use. *See* 350 F.3d at 642-45. Rejecting an argument for two independent reasons does not make either of those reasons dictum. *See Wright v. Spaulding*, 939 F.3d 695, 701 (6th Cir. 2019) (court's "holding" includes reasons "*sufficient* to support the judgment but not strictly necessary in light of an *independent* and equally sufficient conclusion"); *NRDC v. NRC*, 216 F.3d 1180, 1189 (D.C. Cir. 2000) ("[W]here there are two grounds, upon either of which an appellate court may rest its decision, and it adopts both, the ruling on neither is obiter dictum, but each is the judgment of the court, and of equal validity with the other.").

At any rate, whether technically dictum or not, the *WIREdata* decision is at the very least "considered dictum" that accounts for "all the relevant considerations and adumbrates an unmistakable conclusion." *Reich v. Continental Cas. Co.*, 33 F.3d 754, 757 (7th Cir. 1994). It is "ordinarily" "the duty of a lower court to be guided by" such considered dictum. *Id.*; *see Pittman v. Chi. Bd. of Educ.*, 860 F. Supp. 495, 508 (N.D. Ill. 1994) ("[C]onsidered dictum is to be followed as well as a precise holding."), *aff'd*, 64 F.3d 1098 (7th Cir. 1995).

The only other ground Defendants provide for disregarding *WIREdata* is that courts in *other* circuits have supposedly imposed additional requirements on a fair use defense based on intermediate copying that Authenticom cannot meet. *See* Reynolds Br. 47-48 (citing decisions of the Ninth and Federal Circuits). Defendants are incorrect that this non-binding, out-of-circuit authority negates a fair use defense here. Unlike in *Atari Games Corp. v. Nintendo of America Inc.*, 975 F.2d 832 (Fed. Cir. 1992), there is no evidence that Authenticom obtained copies of Reynolds's DMS software through false pretenses. *See id.* at 836, 843 (no fair use when copyrighted material obtained from Copyright Office by false representations); ACOM RSUF 27 (obtained Reynolds's DMS software as the agent of a dealer authorized to use that software). Authenticom's use of Reynolds's DMS software was necessary to provide automated data integration; the manual means available through Dynamic Reporting are no substitute. *See* ACOM SUF 27. And Authenticom used the software to provide data integration services, not in a way that diminished the value of Reynolds's DMS software licensed to dealers. *See WIREdata*, 350 F.3d at 645; *Evolution, Inc. v. SunTrust Bank*, 342 F. Supp. 2d 943, 956 (D. Kan. 2004) (extracting data from database "will have no effect on the potential market" for the database).[50]

III. Defendants' Counterclaims Are Partially Time-Barred

CDK and Reynolds may recover damages only for acts alleged to have occurred within the applicable limitations periods for their respective federal and state law counterclaims. The statute of limitations for CDK's and Reynolds's federal counterclaims runs backward from June 29, 2018 – the date each defendant filed its counterclaims against Authenticom – and the statute of limitations for their state law counterclaims runs backward from May 1, 2017 – the date Authenticom filed its complaint. *See* Auth. Br. 60-62. The Court should therefore bar Defendants' claimed damages outside of each claim's respective limitations period.

Defendants concede the appropriate limitations period for their state law counterclaims. CDK Br. 55; Reynolds Br. 52. But they argue that their federal counterclaims – that is, their DMCA, CFAA, DTSA, and Copyright Act claims – run backward from May 1, 2017, because they are compulsory and "relate back" to the Authenticom complaint. CDK Br. 55-56; Reynolds Br. 52-55. Defendants are wrong for two independent reasons.

[50] Defendants' discussion of the statutory fair use factors in 17 U.S.C. § 107 is beside the point because *WIREdata* compels the conclusion that fair use applies under the facts presented here. In any event, these factors do support a fair use defense for the reasons explained in Authenticom's opposition to Reynolds's motion for partial summary judgment. *See* Dkt. 1081, at 7-8.

First, as explained in Authenticom's brief (at 63), there is no "relation back" doctrine for compulsory counterclaims. Courts adopting such a doctrine erroneously relied on Rule 15, which by its terms applies only to an "amendment to a pleading." Fed. R. Civ. P. 15(c). Rule 13(a), not Rule 15, governs compulsory counterclaims. And, unlike Rule 15, Rule 13 does not provide for relation back. *See* 6 Charles A. Wright et al., *Federal Practice and Procedure* § 1419 (3d ed. 2010). Absent any textual authorization in Rule 13(a), tolling is inappropriate. *See Bus. Guides, Inc. v. Chromatic Commc'ns Enters., Inc.*, 498 U.S. 533, 540-41 (1991); *see also N. Cypress Med. Ctr. Operating Co. v. Cigna Healthcare*, 781 F.3d 182, 206 (5th Cir. 2015). Reynolds's suggestion (at 52) that the Seventh Circuit has endorsed the contrary view reads far too much into *Asset Allocation & Management Co. v. Western Employers Ins. Co.*, 892 F.2d 566, 571 (7th Cir. 1989), which merely observed that other courts have applied a tolling rule in the Rule 13 context; it did not endorse that rule.[51]

Second, Defendants' federal counterclaims are not compulsory. In short, Defendants' counterclaims – all of which, in essence, attempt to fault Authenticom for allegedly unlawful DMS access – might be considered "technically related" to the subject matter of Authenticom's antitrust lawsuit, but they are based on different theories and raise different legal and factual issues. *In re DMS Antitrust Litig.*, 2019 WL 4166864, at *7 (N.D. Ill. 2019) (quoting *Simon v. Nw. Univ.*, 2017 WL 25173, at *3 (N.D. Ill. 2017)). This Court has already applied nearly identical reasoning to conclude that CDK's CFAA counterclaim against the dealership class was not compulsory. *See id.* The Court should apply that same reasoning here.

[51] Nor does it make sense for Defendants' counterclaims – even compulsory counterclaims – to relate back to the filing of *Plaintiff's* complaint. Indeed, nothing prevented Reynolds from asserting its counterclaims before Authenticom filed its complaint, so there is no justification for tolling its counterclaims on the basis of Authenticom's complaint.

Reynolds spills much ink arguing that certain facts relevant to its counterclaims bear some relation to the allegations in Authenticom's complaint. But, as this Court held, just because Authenticom's claims and Defendants' counterclaims share a common origin and overlapping facts does not mean that those counterclaims are compulsory. *See id.* Authenticom's antitrust claims – like the dealership class's essentially identical antitrust claims – are factually and legally distinct from Defendants' counterclaims regarding unauthorized system access. To take just one obvious example: Authenticom's antitrust claims depend upon a broad array of evidence that Reynolds and CDK conspired to stop competing with one another on DMS openness and thereby eliminate competition in the data integration market. *See* Dkt. 1100, at 8-33. The host of factual issues involving those allegations are not at all relevant to Defendants' counterclaims. And whereas the counterclaims turn upon Authenticom's authorization to access the DMS, the antitrust claims do not. In other words, even if Defendants were entitled to deny certain parties access to their DMS generally, they are "not free to withhold such approval pursuant to illegal arrangements." *DMS*, 2019 WL 4166864, at *7.[52]

Third, Reynolds's last-ditch argument (at 56-57) is that its counterclaims relate back to July 2017 – the date of the "Original Counterclaims" it filed in the Western District of Wisconsin prior to its answer (*Authenticom* Dkt. 180) – is also without merit. Reynolds *withdrew* its Original Counterclaims after Authenticom moved to strike that pleading as premature. *See Authenticom* Dkt. 209, at 2 ("Defendant the Reynolds and Reynolds Company's counterclaims, Dkt. 180, are withdrawn. The clerk's office should disregard the entry. Reynolds will refile its counterclaims with its answer."); *see supra* p. 4 (withdrawn pleading is without effect). Accordingly, Reynolds's

[52] Defendants' related argument that their counterclaims are compulsory because they are defenses to Authenticom's antitrust theory is also without merit. This Court already rejected an identical argument in the context of CDK's CFAA claim against the dealership class. *DMS*, 2019 WL 4166864, at *7.

June 2018 counterclaims do not purport to be an amendment to the July 2017 counterclaims. Relation back does not apply.

IV. Defendants' Counterclaims Fail For Additional, Independent Reasons

A. CFAA: Defendants Fail To Show That Authenticom Lacked Authorization Or To Prove Any Single Instance Of Access Caused At Least $5,000 Of Loss

1. Defendants' argument that Authenticom was not authorized to use automated software as the *means* to achieve that access would not establish liability under the CFAA even if the premise were true (which it is not).

a. The CFAA subjects to criminal and civil penalties a person who "intentionally accesses a computer without authorization or exceeds authorized access" and "thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). Although the CFAA does not define "without authorization," the term "exceeds unauthorized access" is defined to mean when a user "*obtain[s] . . . information in the computer that the [user] is not entitled so to obtain*." *Id.* § 1030(e)(6) (emphasis added). Thus, the statutory text focuses on the user's authorization to access and obtain the information at issue.

Construing this statutory text, courts have found that the CFAA does not reach violations of computer-use policies regarding an authorized user's manner of access. In *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012), for example, the Fourth Circuit invoked the rule of lenity (because the CFAA is a criminal anti-hacking statute) to conclude that the CFAA is *not* violated when a user with authorization to access the relevant computer files used unauthorized *means* to achieve that access. The court explained that Congress "has not clearly criminalized obtaining or altering information 'in a manner' that is not authorized. Rather, it has simply criminalized obtaining or altering information that an individual lacked authorization to obtain or alter." *Id.* at 206. Other courts have similarly construed the CFAA.[53]

Here, Defendants' contracts with dealers authorize Authenticom to access the DMS to "obtain" the relevant "information," 18 U.S.C. § 1030(e)(6) – that is, dealer data – as the dealers' agent. Authenticom's authorization to access and use the DMS, and thereby obtain the dealers' data, is dispositive and defeats liability under the CFAA, even if Authenticom violated Defendants' policies with respect to the *manner* it used to obtain that information.

The Seventh Circuit's decision in *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006), does not require a contrary result. That case concerned the definition of "transmission" in the CFAA, *id.* at 419-20, which is not at issue here. Moreover, the defendant had, by his own decision and actions, "terminated his agency relationship" as an employee – which was the basis for his underlying authorization. *Id.* at 420-21. Authenticom's use of software to access dealer data does not terminate its status as a dealer agent (and thus its authorization to access and obtain dealer data). To the extent the Court determines *Citrin* is controlling, we note the Supreme Court has granted certiorari to decide whether the violation of computer-use policies is sufficient to give rise to CFAA liability. *See Van Buren v. United States*, No. 19-783 (U.S.).

b. Hornbook contract law forecloses CDK's argument (at 20-22) that – even if Authenticom had contractual authorization to access the DMS as the dealers' agent – Authenticom remains liable under the CFAA because CDK verbally "revoke[d] any prior consent it may have given." As a matter of contract, CDK authorized dealer agents to access and use the DMS. To

[53] *See, e.g.*, *Valle*, 807 F.3d at 524 (holding that "one 'accesses a computer without authorization' if he accesses a computer *without permission to do so at all*") (emphasis added); *id.* at 526 (construing the CFAA, in light of the rule of lenity, to mean that the relevant "authorization" refers to "the particular computer files or data to which the user's access rights extended"); *Sandvig v. Sessions*, 315 F. Supp. 3d 1, 26 (D.D.C. 2018) ("The focus is on <u>what</u> information plaintiffs plan to access, not on why they wish to access it, the manner in which they use their authorization to access it, or what they hope to do with it.").

revoke that contractual authorization, CDK must modify its contract with dealers, which requires mutual assent. *See* Fenske Ex. 64 (Dkt. 975-64), MSA § 18(A) ("This Agreement shall not be modified in any way except by a writing signed by *both parties*.") (emphasis added). None of CDK's authorities (at 22-23) says a property owner can revoke a bargained-for contractual right of access through unilateral, verbal statements by one party to the contract. Similarly, CDK's argument that its DMS contract confers a license – rather than a property interest in land – misses the point: an intellectual property license, like any other contract, confers binding rights that cannot be changed through unilateral statements.[54]

2. Defendants' position (CDK Br. 46-47; Reynolds Br. 57-63) that they may satisfy the CFAA's loss threshold by aggregating harms caused by distinct CFAA violations conflicts with the statute's language and history. Subclause (I)'s text makes clear that private plaintiffs *may not* aggregate "loss resulting from a related course of conduct affecting 1 or more other protected computers"; that may occur "only" "for purposes of an investigation, prosecution, or other proceeding brought by the United States." 18 U.S.C. § 1030(c)(4)(A)(i)(I). And, although Reynolds is correct (at 61-62) that the statute provides that "loss to 1 or more persons during any 1-year period" may be "aggregat[ed]," that provision permits only aggregation of losses to multiple persons from a single violation; it does not permit aggregation of losses from multiple violations.

Reynolds's assertion that this outcome is absurd (at 63) ignores that it is, as Authenticom showed (at 66-67), the product of a "deliberate legislative compromise": in brief, Congress

[54] CDK's arguments (at 21-22) that requiring it to adhere to its contractual commitments to dealers would "frustrate the purpose of the CFAA" and place it in violation of unnamed "federal data-privacy laws" are unfounded. CDK permitted dealers to use data integrators up until 2015, without incident and certainly without any suggestion that its longstanding business model violated federal law. PJ SAF 22, 71. And still today, every other DMS provider permits dealers to use data integrators, PJ SAF 79, and no data integrator has ever caused a data breach, PJ SAF 16; ACOM SUF 113. In any event, dealers – not DMS providers – are responsible under federal privacy law for the security of consumer data provided to dealers. *See CDK Glob. LLC v. Brnovich*, 2020 WL 2559913, at *7 (D. Ariz. 2020).

permitted the government to aggregate harms across a "related course of conduct," but, for private litigants, it codified the rule of *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 522-23 & n.30 (S.D.N.Y. 2001), that distinct acts could not be aggregated for purposes of satisfying the loss threshold. Reynolds takes issue (at 62 n.55) with *DoubleClick*'s reading of the prior language of the CFAA, but that is beside the point: Congress's adoption of *DoubleClick* dooms Defendants' attempt to aggregate.[55]

Reynolds cites cases reaching a contrary conclusion (at 62 n.55), but those courts were led astray by *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 934 (9th Cir. 2004), the reasoning of which is incorrect for reasons Authenticom has explained (at 67-68). And Defendants' cases interpreting a different statute are beside the point. *See United States v. Yashar*, 166 F.3d 873 (7th Cir. 1999) (addressing 18 U.S.C. § 666); *United States v. Webb*, 691 F. Supp. 1164, 1168 (N.D. Ill. 1988) (same).

Reynolds's argument (at 58-60) that each instance of access produced Reynolds's entire "indivisible injury" also cannot be reconciled with the CFAA's limitations on aggregation. The cases on which Reynolds relies are far afield. Indeed, Defendants cite no case that endorses Defendants' "indivisible injury" rule for purposes of calculating loss under the CFAA.[56]

[55] For what it is worth, some contemporaneous commentators understood the provision just this way. *See* Ronald L. Plesser et al., *USA Patriot Act for Internet and Communications Companies*, Computer & Internet Lawyer (Mar. 2002), https://cyber.harvard.edu/privacy/Presser%20article--redacted.htm.

[56] In *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1066 (9th Cir. 2016), "[i]t [wa]s undisputed that" Facebook's losses exceeded the statutory threshold, and in *Prestige Entertainment West*, 315 F. Supp. 3d at 1173 (a motion to dismiss decision), the propriety of aggregation was likewise not raised. Understandably so: *Creative Computing*'s (incorrect) loss-aggregation rule remains governing law in the Ninth Circuit. And the court in *Svanaco, Inc. v. Brand*, 417 F. Supp. 3d 1042, 1059 (N.D. Ill. 2019), also does not appear to have considered the aggregation question.

B. Trade Secrets: Defendants Fail To Identify An Actionable Trade Secret

No reasonable jury could find in favor of CDK on its counterclaims under the Defend Trade Secrets Act of 2016 and the Wisconsin Uniform Trade Secrets Act because CDK has failed to proffer evidence of any "concrete secrets" that Authenticom allegedly misappropriated. *Composite Marine Propellers, Inc. v. Van Der Woude*, 962 F.2d 1263, 1266 (7th Cir. 1992). After months of discovery, CDK has failed to adduce evidence – in the form of expert opinion or otherwise – to support its vague pleading (at 49) that its DMS's "forms, accounting rules, tax tables, and proprietary tools and data compilations" are actionable trade secrets. Its procedurally improper attempt at this stage to characterize its "DMS as a whole" as a trade secret should be rejected not only because that theory is contrary to its complaint, *see Colbert v. City of Chi.*, 851 F.3d 649, 656 (7th Cir. 2017), but also because the new allegations still fail to identify a concrete secret with adequate specificity.

CDK's opposition fails to fill this evidentiary hole, contending again (at 47-48), vaguely, that the CDK DMS as a whole and, remarkably, all of the data within it (including dealer data) constitute a trade secret. That is, yet again, "not enough" as a matter of law. What is more, the vast majority of information for which CDK now claims protection is undisputedly not even a secret. CDK asserts that the way it "useful[ly]" organizes dealer data and the suite of tools that it employs to do so (which it again never specifies or defines) are protectable – but its thousands of dealer customers, and all of their employees, have ready access to all of that information. CDK can hardly claim protection over a data organizational scheme that it has made no effort to keep confidential from thousands of third parties. *See Fail-Safe, LLC v. A.O. Smith Corp.*, 674 F.3d 889, 893 (7th Cir. 2012) (applying Wisconsin law) (party was not entitled to trade secret protection when it shared that information with a third party).

Similarly, CDK cannot claim that dealer and OEM data is its own trade secret. To constitute a trade secret, a party must derive some independent economic value from the use of that information. *See* 18 U.S.C. § 1839(3)(B); Wis. Stat. § 134.90(1)(c)(1). The dealer data stored on the DMS – dealership customer lists, service and parts inventory, marketing data, and other information – is information from which *dealerships* derive economic value in selling and servicing cars, but that information is not independently useful to *CDK*. And, even assuming it could be, CDK admittedly allows dealers to export that data to any third party through manual methods – so, again, CDK has made no effort to ensure that information is kept confidential. *See Fail-Safe*, 674 F.3d at 893. In *American Family Mutual Insurance Co. v. Roth*, 485 F.3d 930 (7th Cir. 2007), by contrast, the insurance company had a cognizable trade secret in customer information because the company derived independent economic value from that data and made reasonable efforts to keep it confidential. *See id.* at 933. Neither is true for CDK.[57]

CDK's trade secret claims fail for the additional reason that it has no evidence that Authenticom misappropriated "the DMS as a whole." The undisputed evidence is that Authenticom accessed a subset of data stored on the DMS belonging to dealers – data that CDK acknowledges dealerships own (and that is economically valuable to *dealerships*, not CDK) and data that it allows dealers to manually export to whomever they choose. ACOM SUF 26, 109. Though CDK begrudgingly acknowledges these points, it nevertheless claims vaguely (at 49) that Authenticom misappropriated "CDK's proprietary material to organize and display the data in ways useful to dealers." Yet CDK has proffered no evidence that Authenticom misappropriated

[57] CDK's reliance on a similar case, *Duggan v. American Family Mutual Insurance Co.*, 2010 WL 1268175, at *15 (E.D. Wis. 2010), is also inapposite. Again, there, the court concluded that an insurance company could claim trade secret protection over information about its own customers that it stored in a database that it kept confidential from parties outside the company. *Id.*

any organizational scheme (because it has not). Rather, Authenticom takes raw dealer data and organizes that data itself into a more usable format for dealerships and vendors. ACOM SUF 13.

C. UCL: Defendants Impermissibly Seek Damages

Neither Reynolds nor CDK is entitled to damages under the California Unfair Competition Law for alleged "economic injury" because a UCL action is equitable in nature. *See Korea Supply Co. v. Lockheed Martin Corp.*, 63 P.3d 937, 943 (Cal. 2003). Both CDK (at 50) and Reynolds (at 63) concede as much, narrowing their UCL claims to seek solely injunctive relief under the statute.

D. Trespass To Chattels: Defendants Fail To Establish An Actionable Impairment

No evidence supports CDK's and Reynolds's claims that Authenticom caused an impairment to their respective DMS: there is no evidence that Authenticom has suffered or caused a security breach; no evidence that it ever corrupted data on the DMS; and no evidence that it impaired system performance. Without such evidence, Defendants cannot reach a jury on their trespass to chattels claims. *See* Auth. Br. 72-74.

CDK's opposition (at 51) confirms that it relies exclusively upon the testimony of its damages expert, Dr. Rubinfeld, to attempt to prove that Authenticom impaired its DMS performance. [redacted] And, even if that testimony were admissible, it fails to prove that Authenticom's "hits" on the computer system were comparatively large or meaningful, or that they impaired system performance.

Reynolds's opposition also fails to point to any evidence of system impairment. Its argument that it need only prove system access and use to survive summary judgment is unsupported by the two principal authorities upon which it relies: *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 250 (S.D.N.Y. 2000), *aff'd as modified*, 356 F.3d 393 (2d Cir. 2004), and *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000). Both confirm that there must be evidence of diminished system quality or value to prove a trespass to chattels claim. And, in both cases, the plaintiffs could point to such evidence – in *Register.com*, an expert quantified the burden imposed on the plaintiff's computer systems, 126 F. Supp. 2d at 250, and, in *eBay*, a reasonable jury could infer system burden because the defendant admitted to sending 80,000 to 100,000 requests to the plaintiff's computer systems per day, 100 F. Supp. 2d at 1071.

No such evidence exists with respect to Reynolds's trespass to chattels claim. The undisputed evidence shows that Authenticom only caused a system performance issue on the Reynolds DMS one time – an incident in 2009 or 2010, well beyond the statute of limitations – which Authenticom quickly resolved. ACOM SUF 118.[58] Lacking any evidence specific to Authenticom, Reynolds instead points (at 65) to purported "general evidence" about the system burden imposed by independent integrators. But, to survive summary judgment, Reynolds needs concrete evidence that *Authenticom* impaired its system.[59]

E. Unjust Enrichment: Defendants' Claim Is Precluded By Contract

CDK and Reynolds cannot pursue unjust enrichment claims against Authenticom because it is undisputed that their DMS contracts with dealers governed the terms of access to their respective DMS. Contrary to Defendants' principal argument (CDK Br. 53; Reynolds Br. 66-68),

[58] [redacted]

[59] Reynolds's argument that Authenticom's access impaired its customer goodwill is unsupported by any evidence. In fact, the evidence establishes the contrary: that Reynolds's customer goodwill actually suffered as a result of its refusal to allow data integrators' access. PJ SAF 39.

the fact that Authenticom was not a party to those contracts makes no difference. Dealers bargained for data access by their employees *and agents*, and dealers exercised those rights by permitting Authenticom to access the DMS on their behalf. ACOM SUF 53-59, 61-66. If Reynolds and CDK dispute dealers' authorization of Authenticom, their remedy is a breach of contract claim against dealers (which they have pursued) – not an unjust enrichment claim against Authenticom. *See Emirat AG v. High Point Printing LLC*, 248 F. Supp. 3d 911, 936 (E.D. Wis. 2017), *aff'd sub nom. Emirat AG v. WS Packaging Grp., Inc.*, 900 F.3d 969 (7th Cir. 2018); *Gebhardt Bros., Inc. v. Brimmel*, 143 N.W.2d 479, 480-81 (Wis. 1966).[60]

Defendants also argue that their DMS contracts do not bar an unjust enrichment claim here because neither DMS contract authorized *third-party* data access. But, as discussed above, their contracts permitted dealer employees and agents to access their DMS in exchange for substantial licensing fees. ACOM SUF 2-3, 55, 62-63. *Northern Crossarm Co. v. Chemical Specialties, Inc.*, 318 F. Supp. 2d 752 (W.D. Wis. 2004), supports Authenticom because the court rejected an unjust enrichment claim where the subject of the claim (there, marketing efforts) was covered by contract. *Id.* at 766. So too here.

F. Fraud: Defendants Fail To Establish A Misrepresentation Or Reliance

Neither CDK nor Reynolds is able to point to evidence from which a reasonable jury could conclude that Authenticom is liable for fraud.

[60] Reynolds's argument that *Gebhardt* is inapplicable because Authenticom did not "pay" dealers or DMS providers for its access misses the mark. In *Gebhardt*, a subcontractor asserted unjust enrichment against the property owner, but the Court rejected the claim on the ground that the subcontractor had an express contract with the principal contractor. *Gebhardt* thus squarely forecloses Defendants' argument that Authenticom's non-party status precludes it from defending against unjust enrichment on the basis of the DMS contracts. Moreover, it is undisputed that Authenticom performed a service for dealerships when it accessed the DMS; it therefore only benefitted from DMS access in so far as its dealership clients benefitted. DMS providers received compensation for that benefit in the form of the monthly licensing fees dealers paid to their DMS providers. ACOM SUF 2-3.

CDK. CDK's claim, as noted, turns on Authenticom's answer of "Yes" to a DMS login prompt asking if the user was "an authorized dealer employee," and its responses to CAPTCHA prompts. But CDK's MSA expressly permitted dealers' agents to access the DMS on their behalf. CDK therefore cannot claim fraud by unilaterally withdrawing dealers' contractual right to use agents to access the DMS. Nor can CDK establish actual or reasonable reliance to its detriment on Authenticom's answers. The undisputed evidence shows that CDK did not place any actual reliance on the "Yes" answers – it was intended to be "a temporary nuisance" to data integrators. ACOM SUF 100. And, in any event, it knew that Authenticom was answering these prompts.

CDK's principal argument to the contrary (at 53-54) – that Authenticom's representations were false because the prompts were designed to block automated access – ignores the actual text of the prompts. In particular, CDK argues that its Yes/No and CAPTCHA prompts were "intended" to ensure that the user "really was an authorized, human dealer employee." CDK Br. 54. But at no point did the prompts require the user to represent that it was *human* – the prompts simply queried whether the user was *authorized*. And, for the reasons explained, Authenticom plainly was authorized as a dealer agent. CDK attempts to draw a distinction between an "authorized dealer employee" and an "authorized agent" – asserting that, even if Authenticom qualified as an agent, it still falsely represented its status as an "employee." Yet the terms of CDK's MSA draw no distinction between dealers' employees and their agents – it permits both to access the DMS. So even assuming Authenticom's answers were technically misrepresentations, CDK cannot establish that those misrepresentations were material. *See Kaloti Enters., Inc. v. Kellogg Sales Co.*, 699 N.W.2d 205, 211 (Wis. 2005) (intentional misrepresentation claim must involve either a "failure to disclose a *material* fact" or a "statement of a *material* fact which is untrue") (emphases added).

Reynolds. Reynolds's fraud claim rests on Authenticom using dealer-provided login credentials and passwords to access the Reynolds DMS. But the Reynolds login screen did not require Authenticom to make any representation before accessing Reynolds's DMS: it simply prompted entry of a user ID and password. Using valid login credentials – created and provided by dealers – is not a factual representation. And there can be no viable fraud claim in the absence of a representation. *See Grove Holding Corp. v. First Wis. Nat'l Bank of Sheboygan*, 803 F. Supp. 1486, 1503-04 (E.D. Wis. 1992) (under Wisconsin law, claim for fraud requires plaintiff to prove that defendants made a representation of fact).

Reynolds's various arguments to the contrary – that Authenticom allegedly misrepresented itself through the acts of entering login credentials and answering CAPTCHA prompts, or through not disclosing its identity as a data integrator – all suffer from the same critical flaw: Reynolds never prompted users to disclose their automated or human status, or to make a representation regarding any other question, for that matter. Authenticom simply entered login credentials or responded to CAPTCHA prompts to access the Reynolds DMS.[61]

CONCLUSION

Authenticom's motion for summary judgment should be granted.

[61] Both *1st Team Technology, Inc. v. Systems Engineering, Inc.*, 2012 WL 12873551, at *2 (N.D. Fla. 2012), and *United States v. Lowson*, 2010 WL 9552416, at *2 (D.N.J. 2010), are inapt: they involved *stolen* passwords (*1st Team*) and a *criminal* access scheme (*Lowson*).

Dated: August 28, 2020

Respectfully submitted,

/s/ Derek T. Ho

Derek T. Ho
Aaron M. Panner
Daniel V. Dorris
KELLOGG, HANSEN, TODD,
FIGEL & FREDERICK, P.L.L.C.
1615 M Street, NW, Suite 400
Washington, D.C. 20036
(202) 326-7900
dho@kellogghansen.com
apanner@kellogghansen.com
ddorris@kellogghansen.com

Counsel for Authenticom, Inc.

CERTIFICATE OF SERVICE

I, Derek T. Ho, an attorney, hereby certify that on August 28, 2020, I caused a true and correct copy of the foregoing **PLAINTIFF AUTHENTICOM, INC.'S REPLY IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT ON DEFENDANTS' COUNTERCLAIMS** to be filed and served electronically via the Court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the Court's CM/ECF system.

/s/ Derek T. Ho
Derek T. Ho
KELLOGG, HANSEN, TODD,
FIGEL & FREDERICK, P.L.L.C.
1615 M Street, NW, Suite 400
Washington, D.C. 20036
(202) 326-7900
dho@kellogghansen.com